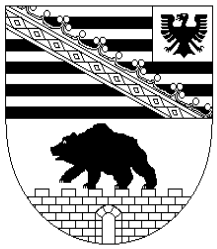
Landesbeauftragter
für den Datenschutz
Sachsen-Anhalt



II. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

**für die Zeit
vom
1. April 1993 bis 31. März 1995**

Inhaltsverzeichnis

Anlagen

Stichwortverzeichnis

Abkürzungsverzeichnis

A

AAÜG	Anspruchs-Anwartschafts-Überleitungs-Gesetz
ADV	Automatisierte Datenverarbeitung
AGE	Automatische Gebührenerhebung
AO	Abgabenordnung
APIS	Arbeitsdatei PIOS - Innere Sicherheit
AuslG	Ausländergesetz
a.F.	alte Fassung

B

BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesarbeitsgericht
BArchG	Bundesarchivgesetz
BAT	Bundesangestelltentarifvertrag
BAT-O	Bundesangestelltentarifvertrag-Ost
BauGB	Baugesetzbuch
BauO LSA	Bauordnung des Landes Sachsen-Anhalt
BDSG	Bundesdatenschutzgesetz (neue Fassung)
BDSG 77	Bundesdatenschutzgesetz (alte Fassung)
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl. I	Bundesgesetzblatt, Teil I
BG LSA	Beamtengesetz Sachsen-Anhalt
BKA	Bundeskriminalamt
BKK	Betriebskrankenkasse
BMI	Bundesministerium des Innern
BND	Bundesnachrichtendienst
BNotO	Bundesnotarordnung
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz
BStatG	Bundesstatistikgesetz
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BZRG	Bundeszentralregistergesetz

D

DEVO	Datenerfassungsverordnung
DONot	Dienstordnung für Notare
DORA	Dialogorientiertes Recherche- und Informationssystem
DÖV	Die öffentliche Verwaltung
Drs.	Drucksache
DSG-LSA	Datenschutzgesetz des Landes Sachsen-Anhalt
DV	Datenverarbeitung

E

ED	Erkennungsdienst
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EStG	Einkommenssteuergesetz
EUROCAT	Europäisches Register über große Fehlbildungen

F

FRV	Fahrzeugregisterverordnung
FVG	Finanzverwaltungsgesetz

G

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

I

IMA-IT	Interministerieller Arbeitskreis IT
INPOL	Informationssystem der Polizei auf Bundesebene
IT	Informationstechnik
ITN-LSA	Informationstechnisches Netz Sachsen-Anhalt
IuK	Informations- und Kommunikationstechnik

K

KAG-LSA	Kommunalabgabengesetz des Landes Sachsen-Anhalt
KAI	Kriminalaktenindex
KAN	Kriminalaktennachweis
KGHB-LSA	Gesetz über die Kammern für Heilberufe Sachsen-Anhalt
KpS	Kriminalpolizeiliche personenbezogene Sammlungen

L

LKA	Landeskriminalamt
LKO LSA	Landkreisordnung des Landes Sachsen-Anhalt
LSA	Land Sachsen-Anhalt

M

MBl. LSA	Ministerialblatt des Landes Sachsen-Anhalt
MDR	Mitteldeutscher Rundfunk
MeldDÜVO LSA	Meldedatenübermittlungsverordnung des Landes Sachsen-Anhalt
MfS	Ministerium für Staatssicherheit
MG LSA	Meldegesetz des Landes Sachsen-Anhalt
MiStra	Anordnung über die Mitteilungen in Strafsachen
MRRG	Melderechtsrahmengesetz

N

NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NUB-Richtl.	neue Untersuchungs- und Behandlungsmethoden
n.F.	neue Fassung

O

OECD	Internationale Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OLG	Oberlandesgericht
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität
OVG	Oberverwaltungsgericht
OWiG	Ordnungswidrigkeitengesetz

P

PC	Personal Computer
PersVG LSA	Landespersonalvertretungsgesetz Sachsen-Anhalt
PKZ	Personenkennziffer
POLAS	Polizeiliche Auskunftssysteme
POLIS	Polizeiliches Informationssystem
ProdGewStatG	Gesetz über die Statistik im Produzierenden Gewerbe
PVS	Personalverwaltungssystem

R

RettDG-LSA	Rettungsdienstgesetz des Landes Sachsen-Anhalt
RuStAG	Reichs- und Staatsangehörigkeitsgesetz

S

Schufa	Schutzgemeinschaft für allgemeine Kreditsicherung
SchwbG	Schwerbehindertengesetz
SGB	Sozialgesetzbuch
SLA	Statistisches Landesamt
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
SPUDOK	Spurendokumentation
StARegG	Gesetz zur Regelung von Fragen der Staatsangehörigkeit
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StUG	Stasi-Unterlagen-Gesetz
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrszulassungsordnung

U

UIG	Umweltinformationsgesetz

V

VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
VermG	Vermögensgesetz
VO	Verordnung
VONot	Verordnung über die Tätigkeit von Notaren in eigener Praxis
VV	Verwaltungsvorschrift
VwVfG	Verwaltungsverfahrensgesetz
VZR	Verkehrszentralregister

W

WoStatG	Wohnungsstatistikgesetz

X

X.25	Protokoll für Datenpaketvermittlung

Z

ZER	Zentrales Einwohnermelderegister (DDR)
ZEVIS	Zentrales Verkehrsinformationssystem
ZPO	Zivilprozeßordnung

Vorbemerkung

Entsprechend seinem gesetzlichen Auftrag legt der Landesbeauftragte für den Datenschutz Sachsen-Anhalt seinen Zweiten Tätigkeitsbericht vor. Der Bericht umfaßt die Zeit vom 1. April 1993 bis zum 31. März 1995 und soll den Abgeordneten des Landtages anhand ausgesuchter Beiträge wiederum einen Überblick darüber geben, wie in allen öffentlichen Bereichen des Landes das in der Verfassung verankerte Grundrecht der Bürger auf informationelle Selbstbestimmung (Art. 6 Abs. 1) beachtet oder weniger beachtet wird. Gezeigt werden soll auch, inwieweit einerseits der Fortschritt auf dem Gebiet der automatisierten elektronischen Verarbeitung personenbezogener Daten mit den Mitteln des Rechts und Maßnahmen der technischen und organisatorischen Sicherheit so im Griff behalten werden kann, daß sich die Elektronik nicht zum Nachteil der Bürger weitgehend verselbständigt, andererseits mit den Mitteln der gleichen Technik aber auch ein ausreichender Schutz für die bei öffentlichen Stellen des Landes vorhandenen umfangreichen personenbezogenen Datensammlungen gewährleistet werden kann.
Auch dieser zweite Bericht ist wieder so verfaßt, daß er neben der Information der Landtagsabgeordneten die Möglichkeit für alle öffentlichen Stellen des Landes bietet, Anregungen und Hinweise für eine eigene datenschutzgerechte Handhabung des Umgangs mit personenbezogenen Daten der Bürger zu erhalten.
Nicht zuletzt sollen die Bürgerinnen und Bürger des Landes in hoffentlich verständlicher Weise darüber aufgeklärt werden, wo überall im Lande sich staatliche Stellen mit ihren personenbezogenen Daten befassen. Vor allem aber sollen sie angeregt werden, sich bei den sie unmittelbar berührenden Verwaltungsdienststellen und Behörden (z.B. Gemeinden, Landkreisen, Schulen und der Polizei) kritisch nach der rechtlich einwandfreien Verarbeitung ihrer persönlichen Daten zu erkundigen und in Zweifelsfällen auch die Hilfe des Landesbeauftragten in Anspruch zu nehmen.

Auch dieser Bericht wird darauf verzichten, Mängel und Fehler einzelner Bediensteter oder bestimmter Dienststellen namentlich aufzuzeigen. Die Erfahrungen der ersten vier Jahre mit dem in Sachsen-Anhalt neuen Recht des Datenschutzes als ein Garant für das Persönlichkeitsrecht jedes einzelnen haben oh-

nehin gezeigt, daß es kaum absichtliche Verstöße gegen dieses Grundrecht gibt, sondern eher Oberflächlichkeit und Sorglosigkeit, manchmal auch falsche Interessengewichtung die Ursache für festgestellte Fehler und Mängel sind.
Der Erste Tätigkeitsbericht hat viel Beachtung bei den öffentlichen Stellen des Landes gefunden und ist bis zum heutigen Tage Ausgangspunkt für viele Nachfragen und Beratungswünsche. Er wird durch diesen Zweiten Tätigkeitsbericht nicht gegenstandslos, sondern setzt die Berichterstattung in vielen Punkten dort fort, wo der erste Bericht aufgehört hat, und er setzt die dort gemachten grundsätzlichen Ausführungen zu den rechtlichen Grundlagen des Datenschutzes im Lande als stille Kenntnis voraus.
Der Landesbeauftragte würde sich deshalb freuen, wenn auch dieser zweite Bericht ein ähnlich brauchbares Mosaiksteinchen im weiteren Bau des Ganzen darstellen würde.

1. Entwicklung des Datenschutzes in Sachsen-Anhalt

Die Entwicklung des Datenschutzes im Berichtszeitraum der vergangenen zwei Jahre ergibt sich zum einen aus den im folgenden abgedruckten Einzelbeiträgen. Zum anderen lassen sich aber einige übergreifende Feststellungen treffen, die auch die wiederkehrenden generellen Probleme öffentlicher Stellen beim Umgang mit dem Grundrecht auf informationelle Selbstbestimmung des Bürgers und dessen technischer und organisatorischer Sicherung aufzeigen sollen.
Zunächst bleibt für den überschaubaren Bereich des Landesgesetzgebers festzuhalten, daß dieser bemüht ist, in enger Abstimmung mit dem Landesbeauftragten bereichsspezifische Regelungen zum Datenschutz zu treffen und damit der anwendenden Verwaltung, wie dem Rat suchenden Bürger, einen festen Anhaltspunkt in der Sachmaterie zu geben.
Sehr viel schwieriger verhält es sich im weiten Aufgabenfeld des Bundesgesetzgebers, der mit seiner Gesetzgebung auch in Sachsen-Anhalt verpflichtende Grundlagen schafft und dabei oft für deren Ausführung durch die Landesverwaltung kaum noch einen Spielraum läßt. Um so wichtiger wäre es, daß auch der Bundesgesetzgeber sich am vom Bundesverfassungsgericht vorgegebenen Ziel

orientieren würde und für die Betroffenen präzise und bereichsspezifische Regelungen in den wesentlichen Rechtsmaterien treffen würde.
Leider läßt sich schon aus den in diesem Bericht enthaltenen Teilbeiträgen herauslesen, daß es da noch große Defizite gibt.

Insgesamt betrachtet läßt sich für alle öffentlichen Stellen des Landes sagen, daß das Stichwort "Datenschutz" grundsätzlich kein fremder Begriff mehr ist. Auch wenn wegen der zugegebenermaßen schwierigen Rechtsmaterie oft nicht die volle Bedeutung und die rechtliche Anwendungsbreite der darunter zu verstehenden vielfältigen Regelungen erkannt werden, wird doch der Zweck des Ganzen (vgl. § 1 DSG-LSA) anerkannt und dessen Bedeutung für den Schutz des einzelnen Bürgers von den Bediensteten im öffentlichen Dienst des Landes weitgehend akzeptiert.
Soweit Einwände aus der Verwaltung heraus geltend gemacht werden, beziehen sie sich meist auf vermeintliche oder tatsächliche Komplikationen oder Störungen im Verwaltungsablauf. Hier ist es nicht nur die Aufgabe des Landesbeauftragten, vermeintliche Komplikationen aufzulösen und in den unvermeidlichen Fällen deutlich zu machen, daß der demokratische Rechtsstaat seine Stärke in erster Linie aus der strikten Beachtung der Grundrechte seiner Bürger und in zweiter Linie aus der zu gewährenden Einzelfallgerechtigkeit gewinnt. Schon deshalb verbieten sich pauschale Betrachtungs- und Behandlungsweisen beim Umgang mit dem Bürger.
Hierzu fehlt es aber häufig auch an der nötigen Erkenntnis der zuständigen Aufsichtsbehörden. Sie nehmen ihre Verantwortung, auf die Einhaltung von Recht und Gesetz (Art. 20 Abs. 3 GG) zu achten, oft nicht oder nicht ausreichend wahr. Das gilt entsprechend für die obersten Landesbehörden und die ihnen speziell nach § 14 Abs. 1 DSG-LSA obliegende Verantwortung. So gehört es zu den klassischen Aufgaben der obersten Landesbehörde, bei erkennbar werdenden Mängeln im Verwaltungsvollzug und auffälligen Rechtsunsicherheiten durch generelle Weisungen eine verbindliche und rechtlich optimale Lösung landesweit sicherzustellen. Wiederholt hat der Landesbeauftragte in diesem Punkt auch zu langsame Reaktionen bei den obersten Landesbehörden beobachtet. Auch allgemeine Anweisungen der Bundesministerien müssen ggf. kurzfristig durch ein

Landesministerium korrigiert werden, wenn sie denn eindeutig als inhaltlich falsch oder rechtsfehlerhaft erkannt worden sind.

Auf der mittleren und unteren Verwaltungsebene wird häufig nicht erkannt, daß die einer Behörde gesetzlich zugewiesene Aufgabe nicht automatisch die gesetzlich erforderlichen Eingriffsregelungen mit umfaßt oder ersetzt. Fehlt eine solche im Spezialgesetz, sind ergänzend (vgl. § 3 Abs. 3 DSG-LSA) die Vorschriften des Gesetzes zum Schutz personenbezogener Daten der Bürger anzuwenden. Dabei hat vor allem das Erforderlichkeitskriterium für die Zulässigkeit einer Erhebung und Verarbeitung der personenbezogenen Daten eine große Bedeutung.
Nicht selten anzutreffen sind auch bei ein und derselben Aufgabenerledigung ein doppelter, ja dreifacher, aber inhaltlich immer gleicher Datenbestand. Ganz gleich, ob hier dieselben personenbezogenen Angaben im Vordruck dreimal durchgeschrieben werden oder im Verwaltungszug dreimal eine eigene Datei angelegt wird - verstoßen wird immer gegen das Verbot der Doppel- und Mehrfacherhebung bei nur einem Zweck.
Übersehen wird häufig in diesem Zusammenhang, daß auch eine auf EDV-Basis durchrationalisierte Leistungsverwaltung im demokratischen Rechtsstaat keine totale Kontrolle aller Leistungsbezieher kennt. Das im übrigen vom Datenschutz nicht in Frage gestellte Prinzip der Ausgabenkontrolle öffentlicher Mittel läßt sich datenschutzgerecht durch den effektiven Einsatz der Rechnungsprüfungsämter und der noch in der Verwaltungspraxis fast unbekannten Geschäftsprüfungen erreichen. Gerade im Bereich der Ausgabenkontrolle benötigt die nächst höhere Aufsichtsbehörde zur Prüfung im Regelfall keine personenbezogenen Auflistungen mit einer Vielzahl von Einzeldaten.

Nach wie vor verbreitet ist auch die bereits vom Bundesverfassungsgericht im sog. Volkszählungsurteil verbotene Vorratsdatenhaltung. So werden oft von den öffentlichen Stellen mehr Daten erhoben als für die konkrete Aufgabe erforderlich sind, oder es werden die für eine bestimmte Aufgabe erhobenen Daten auch nach Erledigung der Aufgabe weiter aufgehoben - man kann sie ja vielleicht noch einmal brauchen. Damit wird aber gegen das alsbaldige Löschungsgebot verstoßen (vgl. § 16 Abs. 2 Nr. 2 DSG-LSA)!

Schließlich bleibt anzumerken, daß die vielfältigen Möglichkeiten der modernen Datenverarbeitungstechnik zwar oft zur rationellen Bewältigung bei der Verarbeitung personenbezogener Daten eingesetzt werden, aber nicht annähernd so häufig für einen effektiven technisch und organisatorischen Schutz (vgl. Ziff. 13) der zu Recht erhaltenen Daten.

Der Landesbeauftragte geht aber davon aus, daß es gelingen wird, die vorstehend aufgezeigte Entwicklung weiter in eine Richtung zu bewegen, die dem Ziel eines sinnvollen und effektiven Datenschutzes im Lande immer näher kommt.

2. Der Landesbeauftragte

2.1 Akzeptanz der Behörde

An dieser Stelle hat der Landesbeauftragte in seinem I. Tätigkeitsbericht (S. 11 ff) eingehend über die rechtliche Stellung und die Aufgaben und Befugnisse seiner Behörde berichtet. Zur Vermeidung von Wiederholungen kann auf diese Ausführungen verwiesen werden.
Es ist deshalb nicht ohne Bedeutung, in diesem Bericht auf die erfreulich hohe Akzeptanz dieser Institution bei den öffentlichen Stellen des Landes hinweisen zu können. Natürlich werden der Landesbeauftragte und seine Mitarbeiter nicht überall gleichermaßen mit freudiger Erwartung aufgenommen, aber deren bisherige intensive Tätigkeit hat fast jeden öffentlichen Tätigkeitsbereich im Lande wenigstens einmal erreicht und in vielen Fällen zu dauerhaften Kontakten geführt, denn die Spezialmaterie Datenschutz berührt fast alle Bereiche staatlichen Handelns.
Insbesondere die beratende Tätigkeit des Landesbeauftragten und der Versuch, mit praxisbezogenen Hinweisen Verbesserungsmöglichkeiten aufzuzeigen, wird überwiegend gerne angenommen und produktiv umgesetzt.

2.2 Geschäftsstelle

Die vorstehend dargestellte Entwicklung hängt auch damit zusammen, daß alle im Haushalt ausgewiesenen Stellen in der Geschäftsstelle des Landesbeauftragten voll besetzt sind. Die meisten Mitarbeiterinnen und Mitarbeiter verfügen nun schon über eine mehrjährige einschlägige Erfahrung in ihrem jeweiligen Tätigkeitsbereich. Im letzten Jahr hat es erstmals je einen personellen Wechsel im Bereich des höheren und des gehobenen Dienstes in zwei Ministerien und von dort zurück gegeben. Auch darin sieht der Landesbeauftragte ein Stück Normalität, das zudem für beide Seiten die Möglichkeit des Erfahrungsaustausches und des gegenseitigen Verständnisses erhöht. Ein solcher Personalwechsel kann und wird sich im angemessenen zeitlichen Abstand im Interesse aller Beteiligter wiederholen.
Für die Bediensteten selbst bietet er die Chance zu neuen Tätigkeitsfeldern und manchmal auch zu einer stellenmäßigen Verbesserung.

Die effektive Arbeitsbewältigung wird auch durch die gute räumliche Unterbringung und eine angemessene Ausstattung mit Haushaltsmitteln gefördert.

2.3 Tätigkeit im Berichtszeitraum

Der Landesbeauftragte und seine Mitarbeiter haben eine stetig zunehmende Zahl von Geschäftseingängen zu bewältigen. Gab es noch im Zeitraum des I. Tätigkeitsberichtes ca. 2.100 schriftliche Geschäftseingänge, so waren es im Jahre 1994 schon fast 2.800; im Zeitraum 1993/1994 betrug die Steigerung 5%. Dazu haben die 10 mit der unmittelbaren Sachbearbeitung befaßten Mitarbeiterinnen und Mitarbeiter und der Landesbeauftragte im Jahre 1994 ca. 850 schriftliche Stellungnahmen erarbeitet.
Zusätzlich bearbeitet werden pro Jahr etwa 650 fernmündliche und eine zweistellige Zahl persönlicher Anfragen.

Die Zahl der Bürgereingaben schwankt zwischen drei und fünf Eingaben pro Woche und hat sich damit auf das Arbeitsjahr bezogen leicht erhöht, liegt aber noch deutlich unter Vergleichszahlen in den alten Bundesländern. Allerdings ist die Zahl berechtigter Eingaben mit gut 30% vergleichsweise hoch.

Formelle Beanstandungen nach § 24 DSG-LSA sind in diesem Berichtszeitraum in 7 Fällen ausgesprochen worden, in etwa 50 weiteren Fällen konnte nach § 24 Abs. 3 DSG-LSA von einer Beanstandung abgesehen werden.
Der Landesbeauftragte hält damit an seiner bisherigen Verfahrensweise fest, wonach nur bewußte, grobe oder hartnäckige Verstöße gegen datenschutzrechtliche Bestimmungen formell beanstandet werden, um den Ausnahmecharakter dieser Maßnahme und das entsprechende Bewußtsein bei den betroffenen öffentlichen Stellen zu erhalten. In einer Vielzahl von Fällen sind nach wie vor Unerfahrenheit in der Verwaltungspraxis und die Unkenntnis der rechtlichen Vorschriften zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten die Hauptursachen für die Mängel.

Die Zahl der von Landesregierung und Landtag erbetenen gutachtlichen Äußerungen liegt im zweistelligen Bereich.

Auch in diesem Berichtszeitraum haben der Landesbeauftragte und seine Mitarbeiter wieder eine Fülle von Beratungsveranstaltungen in allen Bereichen wahrgenommen. Zwei Mitarbeiter unterrichten bei der Aus- und Fortbildung öffentlicher Bediensteter in der allgemeinen Verwaltung und bei der Polizei.

Arbeitsschwerpunkte lagen wie bisher im Sicherheitsbereich, zunehmend liegen sie aber auch im Bereich der Forschung und des Sozialwesens.

Die im I. Tätigkeitsbericht (S. 117 ff) erwähnten Kontrollen bei den Polizeidirektionen und Polizeiinspektionen des Landes wurden abgeschlossen. Anlaßunabhängige neue Schwerpunktkontrollen wurden bei allen Staatsanwaltschaften des Landes, einer Reihe von Einwohnermeldeämtern, Straßenverkehrsämtern, einzelnen Verwaltungsgemeinschaften und in einem Teilbereich des Landesamtes für Verfassungsschutz durchgeführt.

Schließlich haben der Landesbeauftragte und sein Vertreter in einer Vielzahl von Fällen zu Anfragen der Medien Stellung genommen oder von sich aus bestimmte Problembereiche an die Öffentlichkeit in Form von Interviews und Pressemitteilungen herangetragen.

2.4 Zusammenarbeit mit anderen Kontrollorganen

2.4.1 Zusammenarbeit auf Landes- und auf Bund-/Länderebene

Der Landesbeauftragte kann auch hierzu an seine Ausführungen im I. Tätigkeitsbericht (S. 18) anknüpfen.
Eine grundsätzlich gute Zusammenarbeit gibt es mit allen obersten Landesbehörden, die nach § 14 Abs. 1 DSG-LSA jeweils für ihren Geschäftsbereich die Ausführungen der gesetzlichen Vorschriften über den Datenschutz sicherzustellen haben. Allerdings gibt es innerhalb der Häuser in den Abteilungen Unterschiede.
Herausragend gut ist die Zusammenarbeit mit dem Ministerium des Innern. Dies ist nicht nur deswegen von Bedeutung, weil dieses Ressort in der Landesregierung federführend für Grundsatzfragen des Datenschutzrechtes ist, sondern weil in diesem Geschäftsbereich - unabhängig vom Grundsatzreferat 41 und der Zentralen Stelle für Informationstechnik im Referat 34 - allgemeine und spezielle Verwaltungsbereiche beaufsichtigt werden, die für eine Vielzahl von Bürgerinnen und Bürgern Schwerpunkte bei der Verarbeitung ihrer personenbezogenen Daten bilden. Erwähnt seien nur die Meldebehörden, die Polizei und der Verfassungsschutz, aber auch die Bereiche Ausländer-, Archiv- und Vermessungs- und Katasterwesen.
Die schnelle und sachbezogene Zusammenarbeit mit diesem Haus, vor allem aber auch die frühzeitige Unterrichtung und gegenseitige Beratung vermeiden manche Konflikte, die in anderen Bundesländern plötzlich Schlagzeilen machen.

Unverändert sehr gut ist auch die Zusammenarbeit mit dem Landtag. Nicht nur viele einzelne Abgeordnete, sondern auch die parlamentarischen Arbeitsgremien des Landtages und die Landtagsverwaltung wenden sich häufig in Einzel- oder Grundsatzfragen an den Landesbeauftragten. Eine unkonventionelle, gleichwohl konstruktive und vertrauensvolle Zusammenarbeit gibt es bei der Gesetzesberatung in den Fachausschüssen des Landtages.

Ein ständiger Erfahrungsaustausch mit dem Präsidenten des Landtages und Informationsgespräche mit den Vorsitzenden aller im Landtag vertretenen Fraktionen runden die Zusammenarbeit ab.

Die Zusammenarbeit mit dem Bundesbeauftragten für den Datenschutz und den anderen Landesbeauftragten für den Datenschutz im Bundesgebiet hat einen besonderen Stellenwert. Sie wird nicht nur im direkten Kontakt, auf Konferenzen und in Arbeitskreisen kontinuierlich wahrgenommen, weil sie in § 22 Abs. 7 DSG-LSA als besondere Aufgabe vorgegeben ist, sondern weil die Vielzahl vergleichbarer datenschutzrechtlicher Probleme auf der Bund-/Län-derebene die gegenseitige Zusammenarbeit und Unterstützung unabweisbar machen. Die hohen technischen Anforderungen und die Vielzahl bereichsspezifischer Regelungen zwingen nicht nur zur ständigen Information untereinander, sondern auch zur Verteilung von Schwerpunkten bei der Aufgabenerledigung. Gerade eine relativ junge Institution in den neuen Bundesländern kann nicht ohne den mittlerweile 17jährigen Sachverstand vieler fachkundiger Kollegen in den alten Bundesländern auskommen.
Schließlich liegt eine Stärke des föderativen Systems in der Bundesrepublik auch in der Vielzahl kreativer Lösungsmöglichkeiten auf verwaltungsorganisatorischer und rechtlicher Ebene.
Der Landesbeauftragte und seine Mitarbeiter können hier auf allen Zusammenarbeitsebenen nur von sehr guten und bis ins persönliche gehenden Arbeitskontakten berichten.

2.4.2 Zusammenarbeit im europäischen und internationalen Bereich

Besonders erwähnenswert ist abschließend die zunehmend an Bedeutung gewinnende Zusammenarbeit im europäischen und internationalen Bereich. Es liegt auf der Hand, daß insbesondere in Europa anhand der immer engeren wirtschaftlichen, politischen und gesellschaftlichen Verflechtungen auch die Verarbeitung personenbezogener Daten - und hierbei insbesondere die Übermittlung über Landesgrenzen hinweg - ständig zunimmt (vgl. Ziff. 7). Andererseits zeigt sich in der gerade wieder größer gewordenen Europäischen Union deutlich, wie unterschiedlich ausgeprägt die politische Bewertung des Datenschutzes und erst recht ihre rechtliche Absicherung sind. So kann sich beispielsweise als eine Folge der Reiselust der Bürger in Sachsen-Anhalt schnell auch einmal ein Problem

mit der Verarbeitung ihrer Daten in einem Urlaubsland ergeben. Dann ist es vielleicht ganz gut zu wissen, daß dem Landesbeauftragten seit 1994 die Anmeldung einer spanischen Datenschutzkommission aus Madrid vorliegt.

Im Zeitalter von INTERNET und anderen weltumspannenden "Datenautobahnen" wächst das Bedürfnis nach Schutz vor zudringlichen und oft jede Regel des Persönlichkeitsschutzes verletzenden internationalen Datenhändlern und -spekulanten.

Der Landesbeauftragte hat 1994 zum zweiten Mal an einer internationalen Datenschutzkonferenz, diesmal in den Niederlanden, teilgenommen, weil die europäischen und internationalen Konferenzen zum einen den Erfahrungsaustausch über die Vielfalt der weltweit eingesetzten Technik und ihrer Entwicklungen ermöglichen und zum anderen dort Mittel zur technischen und rechtlichen Abwehr unerwünschter Auswirkungen im Bereich der personenbezogenen Datenverarbeitung sachverständig und fachübergreifend diskutiert werden können.
Bei den jährlich stattfindenden Konferenzen sind teilnahme- und stimmberechtigte Mitglieder nur Angehörige staatlich autorisierter Datenschutzkontrollinstitutionen. In der Europäischen Union fehlen noch zwei, im internationalen Bereich nimmt die Zahl der staatlichen Datenschutzinstitutionen von Jahr zu Jahr zu.

2.5 Dateienregister

Das Register der automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert werden, wird seit drei Jahren beim Landesbeauftragten gem. § 25 Abs. 1 DSG-LSA vorgehalten. Es enthält - entgegen der einen oder anderen Vorstellung - keine personenbezogenen Daten der Bürger, sondern soll ihnen die Möglichkeit geben, sich selbst darüber zu informieren, bei welchen der sie interessierenden und für sie zuständigen staatlichen Stellen es welche automatisierten Dateien gibt, in denen sie mit ihren persönlichen Daten gespeichert sind. Leider haben die Bürger bisher davon keinen Gebrauch gemacht.

Daneben nutzt der Landesbeauftragte das Register im Zuge seiner Beratungstätigkeit und im Zusammenhang mit der Durchführung der ihm gesetzlich zugewiesenen Kontrollaufgabe.

2.5.1 Meldeformular zum Register

Nach ersten Erfahrungen mit dem einheitlichen Meldeformular aus dem Jahre 1992 erfolgte 1993 eine Überarbeitung. Dabei wurde insbesondere auf verständlichere Formulierungen in den Hinweisen geachtet.
Außerdem wurde durch die Verfeinerung des Formulars mittels übersichtlicherer Gestaltung die Verwendung vereinfacht.
So kann das Meldeformular neben der Meldung einer automatisiert geführten Datei zum Dateienregister gem. § 25 Abs. 1 DSG-LSA auch zur Unterrichtung über die Einrichtung eines automatisierten Abrufverfahrens gem. § 7 Abs. 4 DSG-LSA und zur Unterrichtung über die Auftragsdatenverarbeitung von Dateien gem. § 8 Abs. 6 DSG-LSA verwendet werden.

Weiterhin können mit ihm Änderungs-, Auflösungs-/Einstellungsmitteilungen oder Sammelmeldungen für automatisiert geführte Dateien erstattet werden.
Der komplette Vordruck trägt auch den verschiedenen Adressaten Rechnung.

Das Meldeformular ist Bestandteil der Verwaltungsvorschrift zum DSG-LSA vom 14.10.1993 (MBl. LSA S. 2485) und dient damit als Kopiervorlage. Außerdem ist es im Excel-Datei-Format verfügbar. Damit ist auch die überall vorhandene PC-Technik nutzbar und der Aufwand zur Erstellung der Dateimeldung wesentlich reduziert.

Für den Polizeibereich wurde, ebenfalls in enger Abstimmung mit dem Landesbeauftragten, die im SOG LSA spezialgesetzlich vorgesehene Errichtungsanordnung im Excel-Datei-Format entwickelt.

2.5.2 Dateienregistermeldungen

Im Jahre 1993 wurden mehr als doppelt so viele Meldungen wie 1994 erstattet. Die Einzelaufteilung für die Jahre 1992 bis 1994 zeigt das Diagramm 1.
Allerdings dürften alle in den Jahren 1992 bis heute eingegangenen Meldungen nur ein Bruchteil der tatsächlich vorhandenen automatisierten Dateien darstellen. Unwissenheit und Trägheit bei den verantwortlichen Stellen sind erfahrungsgemäß die Ursachen dieses Defizits.
Die häufigsten inhaltlichen Fehler sind nach wie vor die unkorrekte Angabe der Rechtsgrundlage für die Verarbeitung und die (fehlende) Regelfrist für die Löschung.

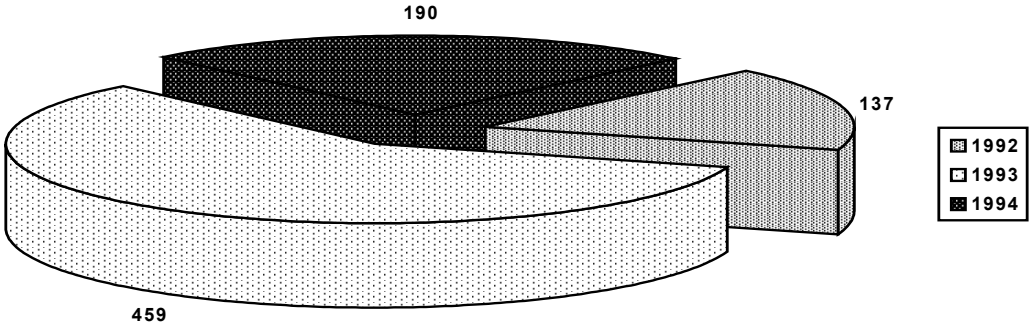


Diagramm 1: Gesamtmeldungen zum Dateienregister der Jahre 1992-1994

Im Diagramm 2 ist das Meldeverhalten der Behörden grafisch dargestellt.

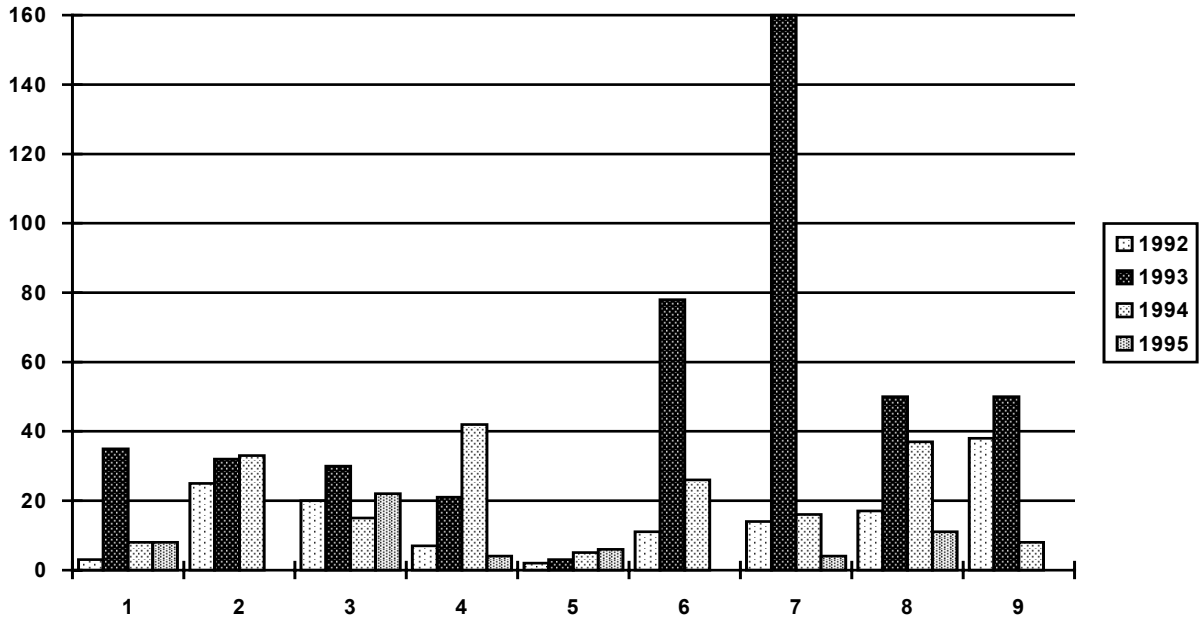


Diagramm 2: Anzahl der Meldungen aus den verschiedenen Behördenebenen (unterteilt in Kalenderjahre)

Aufschlüsselung der Behördenebene:

1 Oberste Landesbehörden
2 Behörden der Mittelinstanz ohne nachgeordnete Bereiche
3 Behörden der Mittelinstanz mit nachgeordneten Bereichen
4 Untere Landesbehörden
5 Landesbeauftragte und sonstige Einrichtungen
6 Kreisfreie Städte
7 Landkreise im Regierungsbezirk Dessau
8 Landkreise im Regierungsbezirk Halle
9 Landkreise im Regierungsbezirk Magdeburg

Aus 18 Landkreisen sind insgesamt 405 Meldungen eingegangen. Aus drei Landkreisen liegt nicht eine Meldung vor.

Von einem der drei Regierungspräsidien wurde lediglich eine Meldung zum Dateienregister erstattet. Es muß jetzt - ebenso wie die drei Landkreise - mit einer nachdrücklichen Mahnung des Landesbeauftragten rechnen.

3. Archivwesen

Die im I. Tätigkeitsbericht (S. 23) dargestellte rechtliche Situation hat sich bisher nicht geändert, die übergangsweise geltenden Rechtsvorschriften haben weiterhin Bestand.
Die auch vom Landesbeauftragten für vordringlich gehaltene Verabschiedung eines Landesarchivgesetzes ist aber ein Stück näher gerückt. Seit Dezember 1994 liegt dem Landtag ein entsprechender Gesetzentwurf der Landesregierung (Drs. 2/383 vom 06.12.1994) vor, der zur Zeit bereits in den Ausschüssen beraten wird, so daß mit einer baldigen Verabschiedung eines Gesetzes gerechnet werden kann.

3.1 Umgang mit personenbezogenen Altdatenbeständen

Auf die Pflicht zur ordnungsgemäßen Aufbewahrung alter Akten und anderer Unterlagen mit personenbezogenen Daten, die in den Verwaltungen nicht mehr benötigt werden, hatte der Landesbeauftragte in seinem I. Tätigkeitsbericht (S. 23) hingewiesen. Trotzdem mußte im Berichtszeitraum festgestellt werden, daß dies weiterhin zu wenig beachtet wird. Dazu sind im folgenden wieder Beispielsfälle dargestellt.
Die in diesem Zusammenhang vom Landesbeauftragten mit Bekanntmachung vom 16. Dezember 1992 (MBl. LSA 1993, S. 523) bei den öffentlichen Stellen abgeforderte Meldung personenbezogener Altdatenbestände ist bis heute in 81 Fällen erfolgt. Es liegt auf der Hand, daß dies bei weitem nicht den noch vorhandenen Beständen entsprechen dürfte.

3.1.1 Unzureichend gesicherte Lagerung

Im April 1993 setzte der ehrenamtliche Bürgermeister einer Gemeinde den Landesbeauftragten davon in Kenntnis, daß personenbezogene Altakten in Kellerräumen der Feuerwehr ohne die einfachste Sicherung gegen unbefugten Zugriff lagerten.

Die örtliche Überprüfung bestätigte nicht nur den dargestellten Sachverhalt, es wurde zusätzlich festgestellt, daß auch auf dem ungesicherten Boden des Hauses der Gemeindeverwaltung Altdatenbestände aufbewahrt wurden.

Die Gemeindeverwaltung hatte die im Ministerialblatt (MBl. LSA 1993, S. 523) abgedruckten Hinweise des Landesbeauftragten ebenso ignoriert wie die gesetzlich festgelegte Pflicht, solche Unterlagen einem Verwaltungsarchiv zur weiteren Behandlung zuzuführen. Diese Aufgaben obliegen der Gemeinde in eigener Zuständigkeit, weil sie dem eigenen Wirkungskreis zuzurechnen sind.

Der Landesbeauftragten hat die ungesicherte Aufbewahrung und die fehlende Meldung der Altdatenbestände formell nach § 24 Abs. 1 Satz 1 DSG-LSA beanstandet.

3.1.2 Aufbewahrung öffentlicher Unterlagen bei Privaten

Nur mit Hilfe des Landesbeauftragten konnte sich 1994 ein Petent gegen die in der Sache unberechtigte Strafverfolgung wegen angeblicher Vernichtung von Archivgut wehren. Ausgelöst wurde das Verfahren durch die unbegründete Strafanzeige einer Stadtverwaltung, die damit von eigenen Versäumnissen beim sorgfältigen Umgang mit Altakten ablenken wollte.

Die Stadt war bis 1992 Eigentümerin eines Grundstücks gewesen, das zu DDR-Zeiten durch eine soziale Einrichtung genutzt wurde. Nach Auflösung dieser Einrichtung befanden sich zunächst noch Arbeitsräume von Bediensteten des Haupt- und Personalamtes in den Räumlichkeiten, die aber - bis auf ein Stallgebäude, in dem Altschriftgut eingelagert wurde - im August 1991 aufgegeben wurden. Das Altschriftgut wurde nach ordnungsgemäßer Sichtung durch den dafür zuständigen Archivverwalter - bis auf wenige Ordner, die entnommen wurden - als für nicht archivwürdig erklärt. Außerdem verblieben in dem Stallgebäude noch Personalunterlagen, aus denen sukzessive Daten in die neue EDV-Anlage eingespeichert wurden.

Im Juli 1992 verkaufte die Stadt das Grundstück durch notariellen Kaufvertrag an den Petenten „mit allen Rechten und Pflichten, den gesetzlichen Bestandteilen und dem Zubehör“.
Der notarielle Kaufvertrag enthielt keinerlei Hinweise oder Vorbehalte der Stadt bezüglich auf dem Grundstück noch etwa vorhandener Altaktenbestände.
Gleichwohl waren die alten Personalunterlagen der Stadt auch am Tage des Besitzüberganges noch im Stallgebäude gelagert.
Der Petent gestattete in der Folgezeit unentgeltlich und ohne eine rechtliche Verpflichtung das Betreten seines Grundstückes und die übergangsweise Nutzung des Stallgebäudes als Lagerraum aufgrund mündlicher Absprache mit einer einzelnen Bediensteten.

Im November 1992 erteilte der Landkreis die Abbruchgenehmigung für das Stallgebäude. Die Abbruchgenehmigung wurde auch der Stadtverwaltung übersandt.
Der Petent ließ den Stall durch eine Baufirma im April 1993 abreißen.
Mitte Mai 1993 stellten Bedienstete des städtischen Haupt- und Personalamtes fest, daß das alte Stallgebäude, einschließlich der dort noch immer gelagerten Restunterlagen, nicht mehr vorhanden war.

Der Landesbeauftragte hat - auch nach Prüfung vor Ort - festgestellt, daß es sich bei den vernichteten personenbezogenen Unterlagen um dienstliches Schriftgut der Stadt gehandelt hat. Diese trug nach den geltenden Rechtsvorschriften die Verantwortung entweder für eine ordnungsgemäße Vernichtung der nicht mehr erforderlichen Altaktenteile oder für die geordnete Aufbewahrung der noch benötigten Unterlagen.
Spätestens beim uneingeschränkten Verkauf und bei der Übergabe des Grundstückes an den neuen Eigentümer im Juli 1992 hätten deshalb entweder vertragliche Regelungen zur weiteren Aufbewahrung des Schriftgutes am bisherigen Lagerort oder aber der unverzügliche Abtransport der Unterlagen in das unmittelbare Gewahrsam der Stadt veranlaßt werden müssen. Die später von einer Bediensteten der Stadt getroffene mündliche Absprache mit dem Eigentümer war aus mehreren Rechtsgründen rechtlich unwirksam und unbeachtlich.

Die Stadt zog ihre Strafanzeige zurück und die Staatsanwaltschaft hat das Verfahren gegen den Betroffenen - nicht zuletzt aufgrund der datenschutzrechtlichen Feststellungen des Landesbeauftragten - als nicht im öffentlichen Interesse liegend eingestellt.

3.2 Mikrofilme über Einreiseanträge von Bundesbürgern

Der Landesbeauftragte hatte durch Zeitungsveröffentlichungen im März 1993 davon Kenntnis erhalten, daß in Halle 136 Mikrofilme aus Beständen der DDR-Volkspolizei aufgetaucht waren. Die Mikrofilme enthielten Anschriften mit geschätzten 100.000 bis 200.000 Namen von Personen, die aus den Altbundesländern in den alten DDR-Bezirk Halle besuchsweise eingereist waren.
Auf den mikroverfilmten Anträgen waren auf der Vorder- und Rückseite persönliche Angaben der Antragsteller vermerkt, wobei im einzelnen Name, Vorname, Geburtsdatum, Wohnungsanschrift, Grund der Einreise, Name und Anschrift der besuchten Personen enthalten waren.
Das Filmmaterial wurde - wie sich später bei den weiteren Ermittlungen herausstellte - von einem Bürger auf einer Mülldeponie gefunden. Der Finder, der die Filme zunächst Journalisten zum Kauf angeboten hatte, übergab das Material dann wenige Tage später der Polizei. Hierzu mag nicht zuletzt eine Pressemitteilung des Landesbeauftragten beigetragen haben, der darauf hingewiesen hatte, daß auch das unbefugte Ansichnehmen solcher personenbezogener Unterlagen nach § 31 DSG-LSA mit Freiheitsstrafe bis zu 2 Jahren bedroht ist.
Die unverzüglich nach Auffinden des Materials vom Landesbeauftragten vor Ort durchgeführten Nachforschungen sowohl bei der Polizeidirektion Halle als auch beim Einwohnermeldeamt der Stadt ergaben das leider übliche Bild einer schlechten Übergangslösung:
Die Filme gehörten zum Bestand des bis zur Wende von der Volkspolizei geführten Einwohnermeldeamtes. Als diese Aufgabe nach dem 3. Oktober 1990 der Stadtverwaltung Halle zufiel, hätte die übergebende Polizeibehörde die Filme entweder selbst geordnet vernichten müssen, weil diese Datensammlung nach den Bestimmungen des Einigungsvertrages nicht mehr zulässig war und für die weitere Verwaltungstätigkeit auch nicht mehr verwendet werden durfte, oder die Filme hätten an die Stadt Halle als gesperrter Datenbestand übergeben werden

müssen, soweit Anhaltspunkte für die Wahrnehmung schutzwürdiger Interessen durch die Betroffenen bestanden. Statt dessen blieben die Filme unbeachtet in den übergebenen Räumen liegen, bis diese Räume für andere Dienstzwecke benötigt und aus diesem Anlaß leer geräumt wurden. Dabei sind die Kartons mit den Filmen ganz unbedarft auf den Müll gefahren worden.
Der zuletzt verantwortliche Verfügungsberechtigte für die Filme wird bis heute bei den beiden beteiligten Behörden gesucht.

3.3 Auskünfte aus dem Kreisarchiv

Ein Landratsamt wandte sich an den Landesbeauftragten mit der Frage, ob es zulässig sei, archivierte Bilanzen eines reprivatisierten Unternehmens, das zwischenzeitlich Kommanditgesellschaft und volkseigener Betrieb gewesen ist, an die Treuhandanstalt bzw. den jetzigen Firmeninhaber zu übersenden.

Der Landesbeauftragte hat hierzu folgenden Standpunkt vertreten:
Aus datenschutzrechtlicher Sicht bestehen keine Bedenken gegen die gewünschte Auskunftserteilung und die Übersendung entsprechender Kopien der Bilanzunterlagen, wenn dies gegenüber dem rechtmäßigen Eigentümer der heute wieder reprivatisierten früheren Kommanditgesellschaft geschieht. Dem Landratsamt wurde empfohlen, sich von der jetzigen Firma den entsprechenden Bescheid über die rechtswirksame Reprivatisierung vorlegen zu lassen.
Sollte die Treuhandanstalt nach wie vor Eigentümer sein, könnte die entsprechende Auskunft und Übermittlung der Unterlagen in Kopie nur an diese erfolgen.

In diesem Zusammenhang hat der Landesbeauftragte für andere Fälle der Auskunftserteilung angemerkt, daß die zur Zeit noch geltende Zweite Durchführungsbestimmung zur Verordnung über das Staatliche Archivwesen der DDR vom 16. März 1976 insofern nicht mehr mit dem Grundgesetz in Einklang steht, als Auskünfte zur "Sicherung gesellschaftlicher Interessen" verweigert werden. Auch die Verweigerung im Hinblick auf "staatliche Interessen" ist nach heute

geltendem Recht nur noch in wenigen spezialgesetzlich geregelten Fällen möglich. Uneingeschränkt Fortgeltung haben dagegen schutzwürdige Belange betroffener Privatpersonen.

4. Ausländerangelegenheiten

4.1 Ausländergesetz

In seinem I. Tätigkeitsbericht (S. 30 f) hatte der Landesbeauftragte darauf hingewiesen, daß das neue Ausländergesetz (AuslG) des Jahres 1990 in § 104 den Erlaß allgemeiner Verwaltungsvorschriften durch das Bundesministerium des Innern (BMI) vorsieht, um eine einheitliche Behandlung der Ausländerangelegenheiten in allen Bundesländern zu gewährleisten.
Diese Verwaltungsvorschriften fehlen bis heute.

Das BMI kann auch derzeit keinen Termin nennen, wann mit einem die §§ 75 bis 80 AuslG betreffenden Entwurf der Verwaltungsvorschriften zu rechnen ist.
Der Landesbeauftragte hält dennoch an der einvernehmlich mit dem Ministerium des Innern des Landes gefundenen Lösung fest, in Sachsen-Anhalt die allgemeinen Verwaltungsvorschriften des Bundes abzuwarten, anstatt die als Entwurf des BMI vorliegenden datenschutzrechtlich sehr bedenklichen vorläufigen Hinweise zu den §§ 76 und 77 in die Landespraxis zu übernehmen.

4.2 Gesetz über das Ausländerzentralregister

Zum 01. Oktober 1994 ist das (Bundes-) Gesetz über das Ausländerzentralregister (AZR-Gesetz) in Kraft getreten. Damit ist nach über 40 Jahren endlich eine gesetzliche Grundlage für die Führung des Ausländerzentralregisters beim Bundesverwaltungsamt in Köln geschaffen worden, nachdem die Datenschutzbeauftragten des Bundes und der Länder in den vergangenen Jahren immer wieder darauf hingewiesen hatten, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem Deutschen wie Ausländern gleichermaßen verfassungsrechtlich garantierten Recht auf informationelle Selbstbestimmung nicht vereinbar sei.

Das Ausländerzentralregister enthält Daten zu mindestens 8 Millionen Ausländern, die sich in der Bundesrepublik Deutschland aufhalten oder aufgehalten haben. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Personen insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Obwohl das AZR-Gesetz gegenüber seinen früheren Entwürfen einige Verbesserungen enthält, bleibt inhaltlich äußerst bedenklich, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dient, sondern darüber hinaus als Informationsverbund für die Polizei, die Strafverfolgungsorgane und die Nachrichtendienste zur Verfügung steht.
Damit wird nicht nur ein altes Trennungstabu durchbrochen, sondern die vom Bundesverfassungsgericht stets für solche außergewöhnlichen Regelungen geforderte Erforderlichkeit und die Verhältnismäßigkeit der Mittel dürften nicht gewahrt sein.

Den Sicherheitsbehörden stehen - worauf die Gesetzesbegründung selbst hinweist - für die Gefahrenabwehr und die Kriminalitätsbekämpfung **eigene** Informationssysteme zur Verfügung.

Es gilt deshalb unverändert die Forderung aus dem Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 09./10. März 1994 **(Anlage 4),** wonach die Speicherung von Erkenntnissen und Ersuchen dieser Behörden nicht in das AZR gehören.

4.3 Ausländerdateienverordnung

Die am 1. Januar 1991 in Kraft getretene Verordnung über die Führung von Ausländerdateien durch die Ausländerbehörden und die Auslandsvertretungen (AuslDatV) schreibt - auch nach Auffassung der Innenministerien des Bundes und der Länder - **verbindlich** vor, welche Dateien die Ausländerbehörden bundeseinheitlich zu Such- und Auskunftszwecken zu führen haben und bestimmt insoweit **abschließend,** welche Daten in diese Dateien aufzunehmen sind.

Auch die Datenschutzbeauftragten des Bundes und der Länder, die sich seit langem für eine solche präzise, bereichsspezifische Regelung eingesetzt hatten, in der der Betroffene - wie es das Bundesverfassungsgericht vorgibt - genau nachlesen kann, wer was zu welchem Zweck an Daten über ihn wissen darf, waren der Auffassung, damit sei in einem wichtigen Bereich des Verwaltungshandelns alles rechtsstaatlich geregelt. Aber weit gefehlt. Schon Anfang 1993 erschien bundesweit ein amtlicher Vordruck, der weitere Datenangaben vom Betroffenen für die Erstmeldung bei der Ausländerbehörde verlangt, die nicht in der AuslDatV aufgeführt sind.
Auf entsprechende Nachfrage des BfD erklärte es das Bundesministerium des Innern für rechtlich vollkommen unbedenklich, wenn bei der Erstmeldung auch Angaben erfragt werden, die in den §§ 3 und 4 AuslDatV nicht aufgeführt sind.

Dieser eigenartigen Auffassung von Rechtsstaatlichkeit hat der Landesbeauftragte für die Verwaltungspraxis in Sachsen-Anhalt widersprochen. Er hat beim Ministerium des Innern des Landes erreicht, daß die Ausländerbehörden angewiesen wurden, die vier möglichen Angaben zur Staatsangehörigkeit der früheren Ehegatten nicht mehr zu fordern und zu speichern. Für diese Daten besteht weder ein rechtliches noch ein praktisches Erfordernis.

4.4 Meldepflicht bei Auslandsstraftaten von Ausländern

In seinem I. Tätigkeitsbericht (S. 32 f) hatte der Landesbeauftragte seine Rechtsbedenken zur Anwendung der Nr. 35 der Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (RiVASt) dargelegt und das Ministerium des Innern aufgefordert, die Übermittlungen nach dieser Verwaltungsvorschrift einzustellen.

Zwischenzeitlich hat das Ministerium des Innern mitgeteilt, die Landesregierung teile zwar die Auffassung des Landesbeauftragten, Nr. 35 RiVASt selbst begründe keine Rechtspflicht der Ausländerbehörden, doch lasse sich wenigstens eine Befugnis zu diesen Mitteilungen (hilfsweise) aus dem DSG-LSA herleiten.

Dem hat der Landesbeauftragte widersprochen. Er hält die vom Ministerium gewählte Rechtskonstruktion für unzulässig, weil sie für die Betroffenen im Ergebnis zu einem **Grundrechtseingriff** führt, der nicht durch eine verfassungskonforme bereichsspezifische Gesetzesregelung gedeckt ist. Die Regelung ist auch inhaltlich fragwürdig, denn reine Verdachtsmitteilungen sind keine geeignete Entscheidungsgrundlage für einen Rechtsstaat, und in vielen Fällen kann die Staatsanwaltschaft damit keinerlei rechtliche Maßnahmen gegen den Betroffenen ergreifen oder begründen.

Der Landesbeauftragte hat daher vorgeschlagen, eine (bundesgesetzliche) bereichsspezifische Rechtsgrundlage für die erwünschte Datenübermittlung zu schaffen.

5. Ausweis- und Meldewesen

5.1 Änderung des Meldegesetzes

Das Gesetz zur Änderung des Meldegesetzes des Landes Sachsen-Anhalt trat am 1. August 1994 in Kraft. Es schafft eine neue Ausweispflicht für Ausländer bei der Anmeldung in Beherbergungsbetrieben.
Aufgrund des Schengener Übereinkommens vom 16. Juni 1990, das an den gemeinsamen Binnengrenzen der Vertragsstaaten den Abbau der Personenkontrollen und der Kontrollen des mit dem Personenverkehr verbundenen Warenverkehrs mit dem Ziel einer vollständigen Beseitigung der Kontrollen vorsieht, enthält die Änderung des Meldegesetzes ergänzende Regelungen zur Hotelmeldepflicht für Ausländer. Die Schengener Vertragsparteien haben sich verpflichtet sicherzustellen, daß sich Ausländer in Beherbergungsbetrieben durch Vorlage eines gültigen Identitätsdokumentes ausweisen.
Eine derartige Ausweispflicht war bisher weder im Melderechtsrahmengesetz noch im Melderecht des Landes (§ 18 Abs. 2 MG LSA) vorgesehen.

5.2 Regelmäßige Datenübermittlungen der Meldebehörden und innerbehördliche Datenweitergabe

Die neue Verordnung zur Durchführung von regelmäßigen Datenübermittlungen der Meldebehörden in Sachsen-Anhalt (MeldDÜVO-LSA) vom 15.07.1993 stützt sich auf § 32 Satz 1 MG LSA und erlaubt **regelmäßige Datenübermittlungen** an andere öffentliche Stellen, soweit das nicht schon in anderen speziellen Vorschriften des Bundes oder des Landes zugelassen ist.

Die Zulässigkeit einer Daten**weitergabe innerhalb** der Gemeinde regelt sich nach § 29 Abs. 5 MG LSA. Danach dürfen im Rahmen des Erforderlichkeitsgrundsatzes alle in § 22 Abs. 1 MG LSA aufgeführten Daten innerhalb der Meldebehörde weitergegeben werden.

Diese Vorschrift muß aber verfassungskonform angewendet werden, denn das Bundesverfassungsgericht hat wiederholt festgestellt, daß der Grundsatz der informationellen Gewaltenteilung auch innerhalb der Gemeindeverwaltung gilt. Daraus folgt, daß auch innerhalb einer öffentlichen Stelle kein beliebiger Datenaustausch und keine ungeprüfte Weitergabe von Daten zulässig ist.
Eine Datenweitergabe zwischen den Ämtern bzw. Sachgebieten darf nur stattfinden, wenn sie zur Aufgabenerfüllung zwingend notwendig ist und eine Zweckänderung dieser Daten zulässig wäre. Natürlich hilft auch eine Einwilligung des Bürgers.

5.3 Auskunft aus dem Melderegister an Mitarbeiter öffentlicher Stellen

Der Leiter eines Ordnungsamtes bat um Auskunft, welche Anforderungen an mündliche Auskunftsersuchen von Mitarbeitern öffentlicher Stellen zu stellen sind, die sich nur mit ihrem Dienstausweis legitimieren.

Die Zulässigkeit der Datenübermittlung an andere öffentliche Stellen regelt § 29 MG LSA. Danach dürfen den in der Vorschrift aufgeführten Behörden Daten übermittelt werden, wenn diese Behörden im Einzelfall aufgrund einer Rechtsvorschrift berechtigt sind, bestimmte Daten zu erhalten. Die in Absatz 3 Nrn. 1 bis 7

genannten Behörden (z.B. Polizei-, Verfassungsschutz-, Strafvollzugsbehörden) haben die für sie geltenden spezialgesetzlichen Vorschriften zu beachten. Ansonsten stellt das Gesetz keine besonderen Anforderungen zur schriftlichen oder mündlichen Form des Auskunftsersuchens; beide sind zulässig.
Im übrigen hat der Gesetzgeber in den Fällen des § 29 Abs. 3 MG LSA die Verantwortung für die Rechtmäßigkeit des Auskunftsersuchens und seine Durchführung, anders als in den Fällen des Absatzes 2, bewußt auf die dort genannten Behörden verlagert.

Die Meldebehörden dürfen sich aber stets die Personalien des Auskunftsersuchenden und seine Behörde notieren und zusammen mit dem Zeitpunkt und einem Hinweis auf die eingesehenen personenbezogenen Unterlagen **gesondert** und befristet für Prüfzwecke festhalten.
Darüber hinaus steht es in Ihrem Ermessen, in Zweifelsfällen bei der entsprechenden Behörde im Einzelfall nachzufragen, ob der Bedienstete zu Recht tätig wird.
Den Meldebehörden bleibt auch die Möglichkeit, den Landesbeauftragten um Rat zu fragen, wenn im Einzelfall Rechtsbedenken aufkommen.

5.4 Adreßbücher

Wie bereits im Berichtszeitraum des I. Tätigkeitsberichts (S. 39) haben sich wiederum Petenten wegen der Herausgabe eines Adreßbuches in ihrer Gemeinde an den Landesbeauftragten gewandt. Teilweise wurde das Adreßbuch als nicht mehr zeitgemäß und sinnvoll angesehen, teilweise wurde befürchtet, daß die im Adreßbuch genannten Personen mit Werbematerial überflutet werden.
In der Antwort des Landesbeauftragten mußte auf § 34 Abs. 3 MG LSA hingewiesen werden, wonach die Meldebehörde den Adreßbuchverlagen grundsätzlich Vor- und Familiennamen, Doktorgrad und Anschriften sämtlicher Einwohner, die das 18. Lebensjahr vollendet haben, mitteilen darf. Allerdings sieht Absatz 4 der genannten Bestimmung vor, daß jeder betroffene Einwohner der Übermittlung seiner Daten **widersprechen** kann. Damit hat sich der Gesetzgeber zu

einer vermittelnden Lösung zwischen den verschiedenen Interessen entschieden. Es wäre auch eine datenschutzfreundlichere Lösung denkbar gewesen, die beispielsweise den völligen Verzicht eines Adreßbuches vorsieht oder die die Datenübermittlung nur mit vorheriger Einwilligung der Betroffenen zuläßt. Nun ist es Sache der jeweiligen Kommunalverwaltung, Vor- und Nachteile einer solchen Entscheidung verantwortungsbewußt selbst abzuwägen. Keine Kommune ist verpflichtet, sich für ein Adreßbuch zu entscheiden. Auch wenn sie sich dafür entscheidet, bleiben inhaltliche Auswahlmöglichkeiten.

Bei seinen Beratungsbesuchen in den Einwohnermeldebehörden des Landes hat der Landesbeauftragte empfohlen, auf das den Bürgern zustehende Widerspruchsrecht - neben der mindestens einmal jährlich vorgeschriebenen Veröffentlichung - an gut sichtbarer Stelle im Meldeamt hinzuweisen. Außerdem ist jeder Bürger bei einer Neuanmeldung oder Umzugsmeldung auf sein Widerspruchsrecht hinzuweisen.

5.5 Verarbeitung kirchlicher Daten im Einwohnermeldeamt

Ein Petent wandte sich mit der Frage an den Landesbeauftragten, ob kircheninterne Karteien mit den Lohnsteuerkarten der Einwohnermeldeämter hinsichtlich des Religionsmerkmals abgeglichen werden dürfen. Gemeint war die entsprechende Datenübermittlung von der Kirche an das Einwohnermeldeamt.

Die Zulässigkeit der Übermittlung personenbezogener Daten von Kirchen an staatliche Behörden fällt nach bundesdeutschem Recht in den Verantwortungsbereich der Kirchen und kann deshalb nur dort überprüft werden. Dafür zuständig sind die Datenschutzbeauftragten der Kirchen. Insoweit wurde der Petent gebeten, sich an seinen zuständigen kirchlichen Datenschutzbeauftragten zu wenden.

Im Rahmen der Zuständigkeit des Landesbeauftragten wurde jedoch geprüft, ob das Einwohnermeldeamt die von der Kirche übermittelten Daten verarbeiten, d.h. im Melderegister speichern durfte, denn auch dies geht nur auf gesetzlicher Grundlage.

Die Gemeinden haben gem. § 39 Einkommenssteuergesetz den unbeschränkt einkommenssteuerpflichtigen Arbeitnehmern für jedes Kalenderjahr unentgeltlich eine Lohnsteuerkarte auszustellen. Dazu sind sie nach § 22 Abs. 1 Nr. 11 i.V. mit Abs. 2 Nr. 6 MG LSA berechtigt, die Zugehörigkeit zu einer Religionsgesellschaft für die Ausstellung einer Lohnsteuerkarte als Merkmal zu speichern, sobald Ihnen vom Betroffenen selbst oder von den zuständigen kirchlichen Stellen die Zugehörigkeit zu einer Religionsgemeinschaft mitgeteilt wird. Mithin war die Speicherung des Religionsmerkmals durch das Einwohnermeldeamt datenschutzrechtlich nicht zu beanstanden. Ein Problem bleibt aber die Eintragung auf der Lohnsteuerkarte (vgl. Ziff. 9.3.2).

5.6 Nähere Bezeichnung des Geburtsortes bei im Ausland geborenen Personen

Nach § 1 Abs. 2 Satz 2 Personalausweisgesetz und der insoweit gleichlautenden Bestimmung des § 4 Abs. 1 Satz 2 Paßgesetz enthält der Ausweis/Paß neben dem Lichtbild des Ausweis-/Paßinhabers und seiner Unterschrift unter Nr. 5 **ausschließlich** Angaben über Tag und Ort der Geburt des Betroffenen.

Bei im Ausland geborenen Personen wird im Paß und Personalausweis zusätzlich zum Geburtsort auch der Staat angegeben, in dem der Einwohner geboren ist. Die Eintragung des Geburtsortes beruht auf Verwaltungsvorschriften der Länder.

Der Landesbeauftragte hat dazu gegenüber dem Ministerium des Innern des Landes Sachsen-Anhalt folgende Auffassung vertreten:

Der Gesetzgeber hat mit seiner Regelung eindeutig zum Ausdruck gebracht, daß er weitere Zusätze zum Geburtsort sowohl im Ausweis als auch im Paß nicht für erforderlich hält. Eine verwaltungsinterne Regelung hat sich bekannterweise an den Vorgaben des Gesetzgebers zu orientieren, jedenfalls kann sie vom betroffenen Bürger keine **zusätzlichen** Angaben fordern.

Aber auch aus sachlichen Gründen erscheint eine weitere Angabe zum Geburtsort im Ausweis/Paß selbst nicht zwingend. Die Feststellung der Person ist

anhand eines gültigen Passes oder Personalausweises mit den vom Gesetzgeber über die Person vorgesehenen Angaben gem. § 1 Abs. 2 Nr. 1-9 Personalausweisgesetz bzw. § 4 Abs. 1 Nr. 1-10 Paßgesetz im Regelfall ohne weiteres möglich. Lediglich in Einzelfällen, in denen die Identifizierung des Ausweisinhabers, z.B. wegen des Verdachts einer Fälschung, nicht hinreichend sicher ist, kann die genaue Bestimmung des Geburtsortes erforderlich werden. Dafür können ggf. zusätzlich im Melderegister gespeicherte Daten oder andere geeignete Urkundsdaten aus dem Personenstandsregister oder Auskünfte des Auswärtigen Amtes herangezogen bzw. eingeholt werden.

Der Bundesgesetzgeber ist aufgefordert, eine einheitliche Handhabung für diese Fälle zu schaffen.

6. Bau- und Bodenrecht

6.1 Datenübermittlung an Baustelleninformationsdienste

Durch eine Bürgereingabe und nach Kontrollen in verschiedenen Bauordnungsämtern wurde dem Landesbeauftragten eine schwunghafte Datenübermittlungspraxis an Baustelleninformationsdienste bekannt.
Die verwendeten freiverkäuflichen Bauantragsformulare verschiedener Verlage im Baugenehmigungsverfahren entsprachen in mehreren Punkten immer dann nicht den datenschutzrechtlichen Anforderungen, wenn der Antragsteller ein privater Bauherr war. Trotzdem übermittelten zahlreiche Bauordnungsämter viele hundert Bauanträge an solche Dienste.

Kernpunkt der datenschutzrechtlichen Beanstandung bildeten Inhalt und Form der rechtlich unzureichend im Vordruck formulierten "Einwilligung" zur Datenübermittlung an Baustelleninformationsdienste.
So war mit der Unterschrift des privaten Bauantragstellers zwar formell die Genehmigung zu einer Datenübermittlung erteilt, eine rechtswirksame Einwilligungserklärung lag aber nicht vor, weil diese in Sachsen-Anhalt in § 4 Abs. 2 DSG-LSA an enge Voraussetzungen geknüpft ist.

Falsch waren auch die "Datenschutzrechtlichen Hinweise" im Formular. Denn weder die geforderten privaten Telefonnummern des Bauantragstellers, seines Vertreters, beteiligter Nachbarn sowie des Entwurfsverfassers noch die Angaben zur Finanzierung gehören zu den nach § 68 des Gesetzes über die Bauordnung des Landes Sachsen-Anhalt erforderlichen Daten bei einem Bauantrag.
Damit war die bisherige Praxis in Teilbereichen der Datenerhebung und bei der Datenübermittlung unzulässig.

Den Bedenken des Landesbeauftragten hat das zuständige Ministerium für Wohnungswesen, Städtebau und Verkehr (MWV) dahingehend Rechnung getragen, daß generell diese „Datenübermittlungsklausel“ aus den für das Land Sachsen-Anhalt in der Ausarbeitung befindlichen landeseinheitlichen Bauantragsformularen entfernt werden soll.
Die Erhebungsdaten in den jetzt vorgelegten Musterantragsformularen bewegen sich im gesetzlich zugelassenen Rahmen und entsprechen damit, bis auf das als freiwillig zu kennzeichnende Datum "Telefonnummer“, den datenschutzrechtlichen Anforderungen.

Eine Umfrage zur Situation in den anderen Bundesländern hat den Landesbeauftragten in seiner Rechtsauffassung bestätigt und ihn bestärkt, an seiner Forderung, die vorgesehenen landeseinheitlichen Bauantragsformulare ohne diese „Datenübermittlungsklausel“ einzuführen, festzuhalten, auch wenn das MWV neuerdings wieder angesichts angeblicher wirtschaftlicher Gesichtspunkte schwankend über die weitere Verfahrensweise geworden ist.

Es ist nicht Zweck des Bauantragsverfahrens Daten für Informationsdienste bereitzustellen, sondern nach Prüfung durch die Bauordnungsbehörde eine Baugenehmigung für das durch den Bauherrn eingereichte Bauvorhaben zu erteilen.
Den Bauordnungsämtern bleibt es unbenommen, bei Vorliegen einer rechtswirksamen Einwilligung des Bauantragstellers, dessen personenbezogene Daten an interessierte Informationsdienste zu übermitteln.

6.2 Datenübermittlung vom Bauordnungsamt an den Mieter

Durch eine Eingabe wurde dem Landesbeauftragten bekannt, daß das Bauordnungsamt eines Landkreises auf Anfrage des Mieters eine Auskunft aus der Bauakte des Vermieters hinsichtlich Baugenehmigung, Schlußabnahme und baurechtlicher Auflage ohne dessen vorherige Kenntnis und Einwilligung gegeben hatte.

Auf die Nachfrage des Landesbeauftragten zur Rechtsgrundlage für die Datenübermittlung stützte sich das Bauordnungsamt auf § 29 VwVfG. Das war falsch. Nach § 29 VwVfG haben nur die Beteiligten Anspruch auf Akteneinsicht. Wer Beteiligter ist, bestimmt sich nach § 13 VwVfG. Der Mieter eines Bauherrn gehört nicht zum Kreis der Beteiligten.

Die Auskunft konnte sich auch auf keine andere gesetzliche Erlaubnis stützen. Das Bauordnungsamt des Landkreises hatte mithin die Auskunft ohne Rechtsgrundlage und damit rechtswidrig erteilt. Wegen dieses nicht unerheblichen Verstoßes gegen datenschutzrechtliche Bestimmungen sah sich der Landesbeauftragte gezwungen, eine förmliche Beanstandung auszusprechen.

6.3 Denkmalschutz

Auch beim Denkmalschutz kann es Probleme mit der Verarbeitung personenbezogener Daten geben. Nach § 18 Denkmalschutzgesetz sind die zuständigen Behörden verpflichtet, ein Denkmalverzeichnis zu führen, in das jedermann Einsicht nehmen darf. Keine eigene Regelung enthält aber das Gesetz, wie dabei mit den Daten der Eigentümer, Besitzer oder Verfügungsberechtigten des Denkmals verfahren werden soll. Diese werden nämlich spätestens dann festgehalten (gespeichert), wenn ihnen die Feststellung der Denkmaleigenschaft formell mitgeteilt wird.

Auf die datenschutzbewußte Anfrage einer Stadt, ob das Denkmalverzeichnis mit den Angaben zum Eigentümer, Besitzer oder Verfügungsberechtigten öffentlich zugänglich gemacht werden dürfe, wies der Landesbeauftragte darauf hin,

daß diese personenbezogenen Daten nicht zugänglich gemacht werden dürfen und deshalb gesondert aufbewahrt werden sollten. Das Einsichtsrecht in das Verzeichnis erlaubt nur die Feststellung der Denkmaleigenschaft, und das im übrigen ergänzend geltende DSG-LSA läßt eine Übermittlung der anderen personenbezogenen Daten nicht zu.

7. Europäischer Datenschutz

7.1 Richtlinie der Europäischen Union

Die Verhandlungen um eine Datenschutzrichtlinie der Europäischen Union zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sind nach langwierigen Verhandlungen unter dem Vorsitz des Bundesbeauftragten für den Datenschutz am 20.02.1995 zu einem ersten Abschluß gekommen. Jetzt muß das Europäische Parlament die Richtlinie billigen. Geschieht dies - ggf. mit Änderungen -, bleibt jedem Mitgliedsstaat zumindest eine Frist von drei Jahren zur Umsetzung in das materielle Recht.

Mit der EU-Datenschutzrichtlinie, die ein wesentliches Element zur Verwirklichung des gemeinsamen Binnenmarktes und damit eines freien Datenverkehrs ist, erreicht der europäische Datenschutz eine neue Qualität, und auch die Staaten außerhalb Europas werden sich an diesem Standard orientieren.
Aus deutscher Sicht ergeben sich durch die Richtlinie unterschiedliche Konsequenzen für den Bereich der öffentlichen Verwaltung und der Privatwirtschaft. Der öffentliche Bereich unterliegt schon jetzt strengeren datenschutzrechtlichen Vorgaben, die sich meist aus bereichsspezifischen Regelungen ergeben. Für die Regelungen des Landes wird die EU-Datenschutzrichtlinie damit voraussichtlich nur wenig Veränderungen bringen, denn durch die konsequente, aber kompromißbereite deutsche Verhandlungsführung konnte das hohe deutsche Datenschutzniveau im öffentlichen Bereich gehalten werden. Es bleibt die endgültige Fassung der Richtlinie abzuwarten. Die Bürger unseres Landes aber können hoffen, daß ihre persönlichen Daten künftig auch außerhalb der deutschen Grenzen besser geschützt werden können.

7.2 Schengener Durchführungsübereinkommen (SDÜ)

Im "Schengener Abkommen" vom 14.06.1985 ist von den Regierungen der Benelux-Staaten, von Frankreich und der Bundesrepublik Deutschland vereinbart worden, die Kontrollen an den gemeinsamen Landesgrenzen schrittweise abzubauen.
Auf der Grundlage dieses Abkommens wurde dann am 19.06.1990 mit den beteiligten Staaten durch einen Staatsvertrag das **"Schengener Durchführungsübereinkommen (SDÜ)"** geschlossen, dem inzwischen vier weitere Staaten (Italien, Portugal, Spanien und Griechenland) beigetreten sind.

Es ist - mit Ausnahme von Griechenland und Italien - am 26. März 1995 in Kraft getreten und hat zum Wegfall der Kontrollen an den gemeinsamen Binnengrenzen geführt.

Aus datenschutzrechtlicher Sicht bedeutsam ist die Verpflichtung der Vertragsparteien, spätestens bis zum Inkrafttreten des Übereinkommens ihr nationales Datenschutzrecht im Hinblick auf die nach dem Übereinkommen übermittelten Daten zumindest dem Standard anzupassen, der sich aus den Grundsätzen des Übereinkommens des Europarates über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.01.1981 ergibt. Außerdem ist die Empfehlung des Ministerausschusses des Europarates für die Nutzung personenbezogener Daten im Polizeibereich vom 17.09.1987 von den Vertragsparteien zu beachten.

Mit der Übermittlung personenbezogener Daten darf erst begonnen werden, wenn in dem Hoheitsgebiet der an einer Datenübermittlung beteiligten Vertragsparteien die im Übereinkommen vorgesehenen datenschutzrechtlichen Regelungen in Kraft getreten sind.

Wesentliche Elemente des nach dem Übereinkommen vorgesehenen Datenschutzes sind:

- der Auskunftsanspruch des Betroffenen,
- die Zweckbindung übermittelter Daten,

- die Verpflichtung, auf die Richtigkeit der Daten zu achten und sie erforderlichenfalls zu berichtigen,
- eine Haftungsregelung hinsichtlich der Geltendmachung von Schadenersatzansprüchen,
- die Pflicht, den Übermittlungsvorgang aktenkundig zu machen und
- die Einrichtung einer unabhängigen Kontrollinstanz bei jeder Vertragspartei, deren Aufgabe darin besteht, den nationalen Datenbestand zu überwachen.

7.2.1 Schengener Informationssystem (SIS)

Ein wichtiger Teilbereich des Schengener Durchführungsübereinkommens mit Auswirkungen auf die Bürger ist das Schengener Informationssystem (SIS). Beim SIS handelt es sich um ein polizeiliches Fahndungssystem, mit dem in allen Schengen-Vertragsstaaten nach Personen oder Sachen durch Ausschreibung gesucht werden kann.

Das Informationssystem besteht aus einem zentralen System (CSIS) mit Sitz in Straßburg und den Teilsystemen (NSIS) der angeschlossenen Vertragsstaaten. Das nationale Teilsystem (NSIS) für die Bundesrepublik Deutschland befindet sich beim Bundeskriminalamt.
Zwischen den Vertragsstaaten findet eine ständige Bestandspflege der von CSIS und NSIS gespeicherten Datenbestände statt, wobei alle Informationen über das zentrale System (CSIS) laufen müssen. Eine direkte Anbindung von Teilsystem zu Teilsystem - also der nationalen Stellen untereinander - besteht nicht.

Für die Ausschreibung zur Suche nach Personen oder Sachen gilt grundsätzlich das Recht des ausschreibenden Vertragsstaates. Ausgeschrieben werden sollen Personen, um deren Festnahme mit dem Ziel der Auslieferung ersucht wird, deren Aufenthalt ermittelt und deren Einreise in einen Vertragsstaat verweigert werden soll. Ebenfalls vorgesehen ist eine Ausschreibung zur verdeckten Registrierung, die innerstaatlich der polizeilichen Beobachtung entspricht, sowie zur vorübergehenden Ingewahrsamnahme für Zwecke der Gefahrenabwehr.

Das Schengener Informationssystem ist zusammen mit den übrigen Teilen des Schengener Durchführungsübereinkommens am 26.03.1995 in Betrieb genommen worden.

7.3 EUROPOL

In dem Vertrag über die Europäische Union (EU) vom 07.02.1992 wurde die Schaffung eines europäischen Polizeiamtes (EUROPOL) vereinbart. Jetzt wird dazu zwischen den Mitgliedsstaaten über eine entsprechende Konvention verhandelt.

EUROPOL soll zunächst die Aufgabe erhalten, bei der Bekämpfung und Verhütung des Terrorismus, des illegalen Drogenhandels, der Geldwäsche, der Nuklearkriminalität, der illegalen Einschleusung und der Bekämpfung der Kfz-Kriminalität als Gemeinschaftseinrichtung Informationen zu liefern.

Bei EUROPOL wird dazu eine zentrale Datenbank als gemeinschaftliches elektronisches Informationssystem eingerichtet, in welches die Mitgliedsstaaten und EUROPOL selbst Daten eingeben und aus der sie Daten unmittelbar abrufen können. Daneben können dort sonstige Dateien für Analyse- und Auswertungszwecke eingerichtet werden.

Die Zusammenarbeit soll über die in jedem Mitgliedsstaat einzurichtende nationale Stelle erfolgen. Diese soll die einzige Verbindungsstelle zwischen EUROPOL und den zuständigen Behörden der Mitgliedsstaaten sein. Die Beziehungen zwischen der nationalen Stelle und den zuständigen innerstaatlichen Behörden unterliegen dem jeweiligen nationalen Recht. In der Bundesrepublik ist als nationale Stelle das Bundeskriminalamt (BKA) vorgesehen.
Da nach bundesdeutschem Recht die Gefahrenabwehr Aufgabe der Länderpolizeien ist, führt diese Rechtskonstruktion nicht nur zu bedenklichen verfassungsrechtlichen Problemen, sondern hat auch Auswirkungen auf die Rechte derjenigen Personen, die durch die Länder zur Gefahrenabwehr im gemeinsam mit dem BKA betriebenen INPOL-System gespeichert sind, wenn das BKA ihre personenbezogenen Daten per Knopfdruck in die EUROPOL-Datenbank weiter übermittelt.

Der Landesbeauftragte hat gegenüber dem Ministerium des Innern wiederholt zu den bisherigen Entwürfen einer EUROPOL-Konvention Stellung genommen und dabei auch vor einer Abkopplung der Länder von ihrer materiellen datenschutzrechtlichen Verantwortlichkeit für ihre Daten gewarnt. Sind diese Daten erst einmal in der EUROPOL-Datenbank, sind ihre weitere Nutzung und die Übermittlung (unter Umständen auch ins internationale Staatengefüge) nicht mehr kontrollierbar und die Auswirkungen für die Betroffenen unkalkulierbar. Dies betrifft nicht nur tatsächliche oder vermeintliche Straftäter, sondern auch "harmlose" Bürger, die als Zeugen, Kontaktpersonen oder Opfer in die Mühlen der europäischen Datenmaschinerie geraten. Die Auskunfts- und Löschungsrechte dieses Personenkreises sind für die Betroffenen bisher kaum überschaubar und nur schwer und umständlich durchsetzbar geregelt. Damit tritt für sie datenschutzrechtlich eine erhebliche Verschlechterung ein. Ob dies mit deutschem Verfassungsrecht noch vereinbar ist, ist fraglich und muß seitens der verantwortlichen Bundesländer, also auch durch Sachsen-Anhalt, noch sorgfältig geprüft werden.
Ein Übergang der datenschutzrechtlichen Verantwortlichkeit von den Ländern auf EUROPOL würde eine eigenständige polizeiliche Aufgabe für EUROPOL schaffen, zu der weder der Bundesgesetzgeber noch die Europäische Union verfassungsrechtlich legitimiert sind.

Bedenklich sind vor allem die vorgesehenen Regelungen zur Übermittlungsbefugnis von EUROPOL an Drittstaaten oder andere Dritteinrichtungen. Die Verleihung solcher Befugnisse und Zuständigkeiten wird nicht durch den EU-Vertrag gedeckt. Die polizeiliche Zusammenarbeit von EUROPOL bezieht sich **ausschließlich** auf die Unterzeichnerstaaten des EU-Vertrages. Nach dem Konventionsentwurf soll aber die datenschutzrechtliche Verantwortung an EUROPOL übertragen werden, ohne daß in bezug auf diese Drittstaaten und Dritteinrichtungen jenseits von EUROPOL ein nachprüfbarer Weg zur Feststellung der Rechtmäßigkeit der Erhebung, Übermittlung, Eingabe sowie der Richtigkeit und Aktualität der Daten erkennbar ist. Insbesondere würde mit diesen Übermittlungsbefugnissen die nach deutschem Recht bestehende materiell-rechtliche datenschutzrechtliche Verantwortlichkeit der Länder für "ihre" Daten aufgehoben.

Auch hinsichtlich der vorgesehenen Regelungen in dem Konventionsentwurf über die Berichtigung und Löschung von Daten, bei denen zwischen EUROPOL und dem eingebenden Mitgliedsstaat Einvernehmen hergestellt werden muß, bestehen Bedenken. Die Einvernehmensregelung führt zu einer Aufhebung der Verantwortlichkeit der Bundesländer für ihre Daten und einer damit einhergehenden Verkürzung ihrer Rechte, denn der Konventionsentwurf sieht vor, daß ein falsches nationales Datum durch den Mitgliedsstaat nur mit Zustimmung von EUROPOL gelöscht werden darf.

Wird der Konventionsentwurf nicht noch in wesentlichen Punkten in den dargestellten Problembereichen geändert, wird der Landesbeauftragte - wie viele seiner Länderkollegen auch - dem Ministerium des Innern nur empfehlen können, personenbezogene Gefahrenabwehrdaten in INPOL nur noch mit der Beschränkung einer ausschließlichen Verwendung im Bundesgebiet einzugeben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer 48. Sitzung einen Beschluß zu den datenschutzrechtlichen Anforderungen an das Übereinkommen gefaßt **(Anlage 9).**

8. Entwicklung der automatisierten Datenverarbeitung

8.1 Automatisierte Datenverarbeitung in der Landesverwaltung

Seit der Darstellung im I. Tätigkeitsbericht des Landesbeauftragten im April 1993 (S. 43) hat die automatisierte Datenverarbeitung den erwarteten breiten Einzug in die Landesverwaltung fortgesetzt.
So hat sich beispielsweise bei einer nur leichten Erhöhung der Beschäftigtenzahl von 1993 auf 1994 die Anzahl der eingesetzten PC um ca. 33% erhöht. Belief sich der durchschnittliche Anteil an PC im Verhältnis zur Beschäftigtenanzahl 1993 auf ca. 42%, ist 1994 eine Erhöhung auf ca. 55% zu verzeichnen. In einzelnen Ressorts liegt der Ausstattungsgrad bei 83 %.
Gleichzeitig war bzw. ist mit der Erhöhung des Ausstattungsgrades eine zunehmende Vernetzung der PC innerhalb der Behörden zu lokalen Netzwerken (LAN = Local Area Network) verbunden. So lag der Anteil der vernetzten PC 1992 noch

unter 1% und beträgt gegenwärtig durchschnittlich ca. 37%. Ressortabhängig reicht die Spannweite bei der Vernetzung von ca. 8 bis 84%.
Zusammenfassend kann man davon ausgehen, daß durchschnittlich jeder zweite Beschäftigte in den Ressorts diese Informationstechnik nutzt und jeder dritte PC innerhalb der Landesverwaltung bereits vernetzt ist.

Dem dargestellten Strukturwandel muß auch das vom Landesgesetzgeber im § 6 DSG-LSA geforderte Datensicherheitskonzept bei jeder öffentlichen Stelle Rechnung tragen. Eine Grundlage für die weitere Inhouse-Vernetzung bildet dabei der gemeinsame Runderlaß des Ministeriums der Finanzen und des Ministeriums des Innern zur landeseinheitlichen Telekommunikations- und Datenverkabelung vom 19.08.1994 (MBl. LSA S. 2237). Die Festlegung des Runderlasses zur gemeinsamen Unterbringung von Etagenverteilern bzw. Verteilerschränken der Telekommunikations- und Datenverarbeitungsnetze in nicht öffentlich zugänglichen Betriebsräumen entspricht den Forderungen des Landesbeauftragten.

In Pilotprojekten, seit Dezember 1994 im Technischen Polizeiamt und seit Februar 1995 im Ministerium des Innern, werden sog. “elektronische Postämter“ (MTA = Message Transfer Agent) eingesetzt, die Erfahrungen aus der Praxis beim elektronischen Dokumentenaustauschverfahren auf der Basis des X.400-Standards von 1988 liefern sollen.
Eine zukünftige Nutzung dieser elektronischen Mitteilungssysteme erfordert aber noch grundsätzliche Regelungen durch die Landesregierung.

Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu auf ihrer 49. Konferenz am 09./10.03.1995 in einer Entschließung auf die Berücksichtigung von Sicherheitsaspekten bei der Nutzung hingewiesen und Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen gegeben, die wesentliche Forderungen zur Gewährleistung eines für alle Bürger ausreichenden Datenschutzes beinhalten **(Anlage 16).**

8.2 Informationstechnisches Netz Sachsen-Anhalt (ITN-LSA)

Auch das im I. Tätigkeitsbericht (S. 43) bereits vorgestellte ITN-LSA wird immer mehr ausgedehnt. Neben dem weiteren Anschluß von Ministerien sind für das Jahr 1995 der Anschluß von Grundbuchämtern der Amtsgerichte, von Finanzämtern und einzelner kreisfreier Städte vorgesehen.
In einem gemeinsamen Runderlaß des Ministeriums des Innern, der Staatskanzlei und der übrigen Ministerien vom 07.02.1994 (MBl. LSA S. 1251) sind die Grundsätze für die Nutzung dieses Landesverwaltungsnetzes durch die Ressorts festgelegt worden. Der Landesbeauftragte wurde bei der Ausarbeitung dieses Erlasses beteiligt. Wer als öffentliche Stelle einen Antrag als Netzteilnehmer stellt und personenbezogene Daten verarbeitet, muß als eine Mindestvoraussetzung ein Datenschutzkonzept gemäß § 6 DSG-LSA für den Anschluß vorlegen können.

Ein noch zu lösendes datenschutzrechtliches Problem stellt die in diesem Netz erforderliche Verschlüsselung personenbezogener Daten durch den einzelnen Netzteilnehmer dar.

Die Verschlüsselung ist notwendig, damit bei eventuellen Zugriffen des Netzmanagements auf die Netzknoten die Vertraulichkeit gewahrt bleibt. Ein weiterer Grund liegt darin, daß im Netzvertrag des Ministeriums des Innern mit der Telecom AG Richtfunkverbindungen, die stark abhörgefährdet sind, zur Datenübertragung vertraglich **nicht** ausgeschlossen sind.
In einigen Bereichen der Landesverwaltung erfolgt die Datenübertragung bereits verschlüsselt.

Der Landesbeauftragte wird über eingereichte Anträge öffentlicher Stellen zum Anschluß an das ITN-LSA informiert und wird bei ihnen im Rahmen seiner Kontrollen die Einhaltung datenschutzrechtlicher Bestimmungen überprüfen.

Beim Ministerium des Innern hat der Landesbeauftragte außerdem seit längerem die Erarbeitung eines Gesamtsicherheitskonzeptes für das ITN-LSA angefordert. Es soll nun erstellt werden.

9. Finanzwesen

9.1 Änderung der Abgabenordnung

Zu diesem Punkt hatte der Landesbeauftragte im I. Tätigkeitsbericht (S. 48) über den vom Bundesfinanzministerium Ende 1992 vorgelegten Gesetzentwurf zur Änderung der Abgabenordnung (AO) berichtet.
Ziel dieses Gesetzentwurfs sollten die Reform des außergerichtlichen Rechtsbehelfsverfahrens nach der AO sowie eine Anpassung der AO an datenschutzrechtliche Vorschriften, insbesondere die Änderung des § 30 (Steuergeheimnis), sein. Eine bessere Ausformulierung datenschutzrechtlicher Belange im Interesse der Steuerbürger hatte auch der Landesbeauftragte gefordert.

Im Juli 1993 wurde aus dem Bundesministerium der Finanzen bekannt, daß weder eine rechtliche noch eine praktische Notwendigkeit für eine Änderung bzw. Ergänzung der AO bezüglich datenschutzrechtlicher Vorschriften gesehen werde.

Die Gegendarstellungen des Bundesbeauftragten und der meisten Landesbeauftragten für den Datenschutz blieben letztendlich erfolglos. Statt dessen wurden durch das Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetz vom 29.12.1993 einige Regelungen in die Abgabenordnung neu aufgenommen, die für die Bürger nicht nur von Vorteil sind und deshalb kurz angesprochen werden sollen:

1. Die für die Verwaltung der Grundsteuer zuständigen Behörden sind nun berechtigt, die aufgrund des Steuergeheimnisses (§ 30 AO) geschützten Namen und Anschriften von Grundeigentümern, die bei der Verwaltung der Grundsteuer bekanntgeworden sind, zur Verwaltung anderer Abgaben sowie zur Erfüllung sonstiger öffentlicher Aufgaben zu verwenden. Sie dürfen diese Daten den hierfür zuständigen Gerichten, Behörden oder juristischen Personen des öffentlichen Rechts auf Ersuchen mitteilen. Dies gilt nicht, soweit überwiegend schutzwürdige Interessen des Betroffenen entgegenstehen (§ 31 Abs. 3 AO).

2. Die Finanzbehörden dürfen Sozialleistungsträgern und Subventionsgebern Tatsachen mitteilen, die zur Aufhebung von deren Leistungsbescheiden und zu Erstattungen von Sozialleistungen und Subventionen führen können (§ 31a Abs. 3 AO).

3. Die Finanzbehörden dürfen die durch das Steuergeheimnis (§ 30 AO) geschützten Daten auch für Zwecke künftiger Steuerverfahren und Steuerstrafverfahren in Dateien oder Akten sammeln und verwenden (§ 88a AO).

Beispielhaft für die bisherige unzureichende und mangelhaft abgestimmte Flickarbeit des Bundesgesetzgebers ist die bereits vorstehend erwähnte neue Einfügung des § 88a. Danach dürfen die Finanzbehörden zwar allerlei personenbezogene Daten sammeln, aber es fehlt noch immer die normenklare gesetzliche Ermächtigung zur Einrichtung der vorgesehenen bundesweit geführten Fahndungsdatei.
Der Landesbeauftragte ist sich deshalb mit seinen Kollegen einig, daß an dem Ziel der komplexen Einfügung datenschutzrechtlicher Vorschriften in die AO festgehalten werden muß. Dabei kann es nicht um die für den Steuerbürger gefährliche Aufweichung der bisherigen Vorschriften über das Steuergeheimnis gehen, sondern um die systematische Neuordnung der vorhandenen datenschutzrechtlichen Vorschriften und die Eingliederung aller Vorschriften über das Erheben, Verarbeiten und Nutzen von Steuerdaten in einem eigenen Abschnitt (z.B. im vierten Teil) der Abgabenordnung.

Auch im sensiblen Bereich des Abgabenrechts muß endlich eine Anpassung an die verfassungsrechtlichen Vorgaben des Bundesverfassungsgerichts erreicht werden.

9.2 Entwurf einer Steuerdatenabruf-Verordnung (StDAV)

Mit dem Steuerbereinigungsgesetz 1986 ist der Schutzbereich des Steuergeheimnisses in § 30 der Abgabenordnung (AO) erweitert worden. Damit besteht nach § 30 Abs. 2 Nr. 3 AO auch ein Schutz gegen den unbefugten Abruf von Daten in automatisierten Verfahren, wenn die Daten in einer Datei gespeichert

sind. Es gibt aber eine für den Datenschutz der Steuerbürger gefährliche Hintertür:
Das Bundesministerium der Finanzen (BMF) kann mit Zustimmung des Bundesrates durch eine Rechtsverordnung bestimmen, ob ein Abruf von Daten im automatisierten Verfahren zulässig sei und welche Amtsträger hierzu ermächtigt werden sollen. Genau dies hat das BMF jetzt getan. Der 1994 nach längeren Vorüberlegungen vorgelegte Entwurf einer StDAV sieht u.a. die Einbeziehung der Möglichkeit von Online-Abrufen durch Rechnungsprüfungsbehörden des Bundes, der Länder und der Gemeinden vor. Der Landesbeauftragte hat gemeinsam mit anderen Datenschutzbeauftragten rechtliche Bedenken gegen die Einbeziehung der Rechnungshöfe geltend gemacht, weil dafür die erforderliche Rechtsgrundlage im Gesetz fehlt. Der gegenwärtige § 30 Abs. 6 der AO kommt nicht als Rechtsgrundlage für die Rechnungshöfe in Betracht, da diese nicht Verfahrensbeteiligte im Sinne von § 30 Abs. 2 Nr. 1 a und b AO sind.

Das BMF hat nun zwar zugesagt, bei der nächsten Änderung der AO den gesetzgebenden Körperschaften eine Ergänzung des § 30 AO vorzuschlagen, will aber trotzdem jetzt schon die Rechnungsprüfungsbehörden zum automatisierten Abruf zulassen - vorläufig ohne Rechtsgrundlage.
Dies ist kein Beispiel rechtsstaatlicher Verwaltung und für die Bürger gefährlich, denn sie wissen jetzt nicht mehr - wie es das Bundesverfassungsgericht fordert -, wer was zu welchem Zweck aus ihren Steuerunterlagen weiß. Denn das datenschutzrechtlich gefährliche am bisherigen automatisierten Abrufverfahren ist der Wegfall der Verantwortlichkeit der Steuerbehörden für ihre Daten und die Tatsache, daß die Steuerbehörden selbst den (heimlichen) Abruf der Steuerdaten gar nicht merken und beeinflussen können. Gegenüber dem bisherigen Rechnungsprüfungsverfahren verschlechtert sich dadurch der Schutz und die Information des Steuerbürgers erheblich.
Der Entwurf der StDAV liegt zur Zeit dem Bundesrat zur Zustimmung vor.

9.3 Kirchensteuermerkmale auf der Lohnsteuerkarte

Nach dem gegenwärtigen Recht ist der Arbeitnehmer gezwungen, seine Konfessionszugehörigkeit und darüber hinaus auch die seines Ehegatten dem Arbeitgeber über die Lohnsteuerkarte zu offenbaren. Das ist aus mehreren Gründen datenschutzrechtlich bedenklich:

9.3.1 Kenntnis des Arbeitgebers von der Konfessionszugehörigkeit

Die verfassungsrechtlichen Grundsätze der Verhältnismäßigkeit und der Gleichbehandlung dürften verletzt sein, denn der Arbeitgeber ist nach höchstrichterlicher Rechtsprechung grundsätzlich nicht befugt, nach der Konfessionszugehörigkeit seines Arbeitnehmers und schon gar nicht nach der seines Ehegatten zu fragen. Dieses Verbot wird durch die Eintragung auf der Lohnsteuerkarte praktisch unterlaufen.
Diesem Angabezwang auf der Lohnsteuerkarte unterliegt nur der Teil der Steuerpflichtigen, der Einkünfte aus nichtselbständiger Arbeit bezieht und lohn- bzw. einkommenssteuerpflichtig ist.

9.3.2 Eintragung der Kirchensteuermerkmale

Für die Eintragung der Kirchensteuermerkmale in die Lohnsteuerkarte fehlt es an einer erforderlichen normenklaren bereichsspezifischen Rechtsgrundlage, die den Eingriff in das informationelle Selbstbestimmungsrecht der Arbeitnehmer für die Betroffenen deutlich erkennbar regelt.
Die landesgesetzlichen Regelungen im MG LSA enthalten zum Inhalt der Lohnsteuerkarte hinsichtlich der Religionszugehörigkeit keine Bestimmungen.

Zwar sind die Arbeitgeber verpflichtet, die Kirchensteuer von allen Kirchenangehörigen mit dem maßgeblichen Steuersatz einzubehalten und an das zuständige Finanzamt abzuführen, doch auch die dafür geltenden Vorschriften des Einkommenssteuergesetzes sagen dazu nichts aus. Lediglich Abschnitt 108 Abs. 9 der Lohnsteuerrichtlinien enthält Anweisungen, denen aber gegenüber dem Steuer-

bürger keinerlei Eingriffsberechtigung zukommt, weil es sich dabei nur um Verwaltungsvorschriften handelt.

Nach jahrelangem Tauziehen mit den Datenschutzbeauftragten haben die obersten Finanzbehörden der Länder nunmehr endlich vereinbart, daß ab 1995 die Kirchensteuermerkmale des Ehegatten bei konfessionsgleichen und glaubensverschiedenen Eheleuten nicht mehr auf der Lohnsteuerkarte eingetragen werden sollen. Bei konfessionsverschiedenen Eheleuten ist die Eintragung weiter erforderlich, solange die einbehaltene Kirchensteuer je zur Hälfte an die Kirche des Arbeitnehmers und des Ehegatten abzuführen ist (Halbteilung der Kirchensteuer).

Die Frage, ob die Halbteilung der Kirchensteuer im Lohnsteuerverfahren aufgegeben werden kann, soll von den Kirchenvertretern erörtert werden, sobald Untersuchungen des Landes Bayern über die Notwendigkeit der Halbteilung dazu abgeschlossen sind.
Das Ergebnis der Untersuchung wird deshalb bundesweit für die künftige datenschutzgerechte Behandlung der Konfessionsdaten der Arbeitnehmer entscheidende Bedeutung haben.

9.4 Eintragung des Freibetrags für Behinderte auf der Lohnsteuerkarte

Nach Beantragung eines Freibetrages für eine Schwerbehinderung gem. § 39a EStG wird von den Finanzämtern automatisch der gewährte Freibetrag an die Gemeinden übermittelt. Die Gemeinden führen daraufhin den Freibetrag in den Folgejahren bei der Ausstellung der Lohnsteuerkarte mit auf. Aus der Angabe des Freibetrages auf der Lohnsteuerkarte kann der Arbeitgeber aber ohne weiteres erkennen, mit welchem Grad der Behinderung sein Arbeitnehmer eingestuft ist. Dies kann für einen behinderten Arbeitnehmer nachteilige Auswirkungen haben, insbesondere solange er noch nicht den verstärkten Kündigungsschutz nach dem Schwerbehindertengesetz genießt.
Es sind aber auch Fälle denkbar, in denen der Steuerpflichtige nicht wünscht, daß die betreffende Gemeinde seine Behinderung durch eine Datenübermittlung

des Finanzamtes erfährt. Dieses kann z.B. in kleineren Gemeinden der Fall sein, wo Gemeindebedienstete und Steuerpflichtige sich persönlich kennen.
Dem Steuerpflichtigen sollte deshalb die Möglichkeit gegeben werden, der Datenübermittlung durch das Finanzamt an die Wohnsitzgemeinde zu widersprechen und die Eintragung des Freibetrages auf der Lohnsteuerkarte über einen jährlichen Antrag auf Lohnsteuerermäßigung zu erreichen.

Das Bundesministerium der Finanzen und die obersten Finanzbehörden der Länder haben sich aus verwaltungsökonomischen Gründen gegen eine solche Wahlmöglichkeit des Steuerpflichtigen ausgesprochen. Es wird befürchtet, daß hierdurch der Weitergabe in einer Vielzahl von Fällen unbegründeterweise widersprochen und so das bisher "bewährte Eintragungsverfahren" beeinträchtigt würde.
Ein angesichts des hohen Stellenwertes des Grundrechtschutzes geradezu lächerliches Argument.
Wenigstens hat man ab 1995 im Abschnitt „Versicherung“ des Vordrucks auf „Lohnsteuerermäßigung“ einen Hinweis auf die erforderlichenfalls mögliche Weitergabe von Angaben über Pauschalbeträge für Behinderte an die für die Ausstellung von Lohnsteuerkarten zuständige Gemeinde eingefügt.

9.5 Zuordnung der Spielbank zum DSG-LSA

Aufgrund einer Eingabe hatte der Landesbeauftragte der Frage nachzugehen, ob die in § 7 Abs. 2 der Spielverordnung für die öffentlichen Spielbanken im Land Sachsen-Anhalt festgelegte Anordnung der Aufsichtsbehörde zur Führung einer Besucherdatei mit dem Datenschutzrecht des Landes im Einklang steht.

Die Spielverordnung für die öffentlichen Spielbanken im Land Sachsen-Anhalt vom 21. April 1993 findet ihre Rechtsgrundlage in § 9 des Spielbankgesetzes vom 26. Juni 1991. Beide Rechtsvorschriften sind sog. bereichsspezifische Regelungen, die für den Spielbetrieb den allgemeinen Vorschriften des Landesdatenschutzgesetzes vorgehen.

Der Landesbeauftragte konnte in einem Punkt erfolgreich beim Ministerium der Finanzen (MF) auf eine verfassungskonforme Handhabung des § 9 Satz 2 Spielbankgesetz hinwirken. Danach ist die Spielordnung auch vor den Spielsälen auszuhängen. Nur so kann sich der Spieler rechtzeitig von den geltenden Rechtsgrundlagen im Spielbetrieb informieren und die möglichen Auswirkungen, z.B. der Speicherung seiner Personalien, überdenken.

Zu unterschiedlichen Rechtsauffassungen zwischen dem MF und dem Landesbeauftragten kam es zu der Frage, ob die in § 7 Abs. 2 der Spielverordnung grundsätzlich zugelassene Besucherdatei - wie jede andere Datei einer öffentlichen Stelle des Landes - gem. § 25 Abs. 1 DSG-LSA dem Landesbeauftragten zum Dateienregister zu melden ist, damit sie interessierte Bürger einsehen können. Das MF will eine solche Meldung nicht abgeben, da nach seiner Auffassung die Spielbank als Gesellschaft des privaten Rechts nicht unter den Anwendungsbereich des DSG-LSA fällt. Folgt man dieser Auffassung, findet auch keine Kontrolle durch den Landesbeauftragten statt.

Der Landesbeauftragte vertritt demgegenüber den Standpunkt, daß es für die Einbeziehung der Spielbank unter die Vorschriften des DSG-LSA nicht darauf ankommt, ob das Land die Spielbank als private Gesellschaft deklariert, sondern nur darauf, ob der Staat tatsächlich Mehrheitsträger ist. Die Personen- und Kapitalgesellschaften des Landes, bei denen das Land die Mehrheiten hält, sind dann unter das DSG-LSA einzuordnen, wenn sie eine öffentliche Aufgabe wahrnehmen. Beide Punkte hat der Landesgesetzgeber bereits entschieden.

Ausgehend von dem gesetzlichen Verbot des privaten Glückspiels läßt das Spielbankgesetz aus Gründen der staatlichen Kontrolle nur **öffentliche** Spielbanken zu (§ 1 Abs. 1 Spielbankgesetz).
Damit handelt es sich um eine öffentliche Aufgabe, und die ausschließlich vom Land gehaltene Spielbank GmbH und Co KG fällt in den Anwendungsbereich des DSG-LSA.

Der Landesbeauftragte hält daher an der Auffassung fest, daß gem. § 25 Abs. 1 DSG-LSA eine Dateiregistermeldung über die Besucherdatei dem Landesbeauftragten vorzulegen ist.

Das MF möchte aber diesen Punkt im Rahmen einer anstehenden Novellierung des Spielbankgesetzes auch noch einmal im Gesetzgebungsverfahren geklärt wissen.

9.6 Hundebestandsaufnahme bei den Grundstückseigentümern für die Hundesteuer

Aufgrund einer Eingabe eines Petenten erfuhr der Landesbeauftragte davon, daß die von einer Stadt erlassene Hundesteuersatzung die Möglichkeit vorsieht, im Wege der Hundebestandsaufnahme bei den Grundstückseigentümern eine Kontrolle der gehaltenen Hunde und deren Halter durchführen zu können.
Zu dieser Satzungsbestimmung hat der Landesbeauftragte der betreffenden Stadt folgende Hinweise gegeben:

- Gegen eine Befragung **aller** Grundstückseigentümer der Stadt bestehen erhebliche datenschutzrechtliche Bedenken, da eine solche generelle Befragung eine unzulässige Steuerfahndung nach unbekannten Steuerfällen darstellt und dabei auch gegen das Übermaßverbot verstoßen wird.
- Die Befragung jedes Grundstückseigentümers ist zudem von der Rechtsgrundlage der Satzung nicht gedeckt, denn diese erlaubt nur die Besteuerung von Hundehaltern; nicht jeder Grundstückseigentümer ist aber Hundehalter.
- Bei einer generellen Hundebestandsaufnahme würden auch die von der Steuerbefreiung oder -ermäßigung nach der Hundesteuersatzung betroffenen Hunde erneut erfaßt. Insoweit läge der Fall einer unzulässigen Doppelerhebung vor.

- Unzulässig wäre auch die Erhebung personenbezogener Daten (Name, Anschrift, usw.) solcher Hundehalter, deren Tiere sich nur besuchsweise oder nur zur Pflege auf einem Grundstück in der betreffenden Stadt befinden und die bereits in anderen Gemeinden versteuert werden und damit nicht der Hundesteuersatzung der Stadt unterliegen.

Diese datenschutzrechtlichen Bedenken lassen sich aber bei rechtskonformer Auslegung und Anwendung der Hundesteuersatzung ausräumen. Dabei muß beachtet werden, daß nicht alle Grundstückseigentümer generell befragt werden dürfen. Nach § 93 Abs. 1 Satz 3 AO sollen andere Personen erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziel führt oder keinen Erfolg verspricht. Von dieser Vorschrift darf nur aus konkreter Veranlassung im Einzelfall bzw. bei einer bestimmbaren Anzahl von Fällen Gebrauch gemacht werden.

9.7 Weiterführung und Ergänzung der Territorialen Grundschlüsseldaten (TGS)

Eine Stadtverwaltung wurde von einem Finanzamt gebeten, eine Aufstellung aller nach dem 01.01.1991 fertiggestellten Wohn- und Geschäftsgebäude und deren Eigentümer mit Fertigstellungsterminen zu übersenden sowie eine künftige vierteljährliche Ergänzung des Territorialen Grundschlüssels (TGS) in dem Verwaltungsgebiet der Gemeinde vorzunehmen.

Das Finanzamt stützte sein Auskunftsverlangen auf § 29 Abs. 3 Bewertungsgesetz, wonach die nach Bundes- oder Landesrecht zuständigen Behörden den Finanzbehörden die ihnen im Rahmen ihrer Aufgabenerfüllung bekanntgewordenen rechtlichen und tatsächlichen Umstände mitzuteilen haben, die für die Festsetzung von Einheitswerten des Grundbesitzes oder für die Grundsteuer von Bedeutung sein können.

Bei dem TGS-Verzeichnis handelt es sich um ein vielschichtiges Verwaltungshilfsmittel der ehemaligen DDR, für das es seit dem 3. Oktober 1990 keine Rechtsgrundlage mehr zur weiteren Erhebung, Verarbeitung und Nutzung personenbezogener Daten gibt. Soweit die Stadtverwaltung noch über alte Aufstellun-

gen zum TGS verfügt, dürfen deshalb von ihr daraus keine personenbezogenen Daten mehr übermittelt werden.

Vielmehr richtet sich die Verwendung der alten TGS-Bestände nach den §§ 33 bis 36 DSG-LSA. Nach § 33 Abs. 1 DSG-LSA sind die Unterlagen an die jetzt dafür zuständigen Stellen abzugeben. Das sind nach einer Entscheidung des Ministeriums des Innern des Landes Sachsen-Anhalt die Katasterämter. Sie müssen anhand der genannten Bestimmungen bei Auskunftsersuchen im Einzelfall prüfen, inwieweit daraus noch zulässigerweise Einzelangaben erforderlich sind.

Das Finanzamt hat sich für Auskünfte an die jetzt zuständigen Stellen zu wenden. Das sind für den Bereich des Liegenschaftswesens die Katasterbehörden, hinsichtlich des Eigentümernachweises die Grundbuchämter und hinsichtlich der Bauantragsteller die Bauordnungsämter der Landkreise.

Im übrigen hatte das Finanzamt übersehen, daß es sich nach der insoweit bindenden gesetzlichen Vorgabe des § 29 Abs. 1 des Bewertungsgesetzes bei Auskünften immer zunächst an die Eigentümer zu halten hat. Nur so wird der auch in Sachsen-Anhalt garantierten Verfassungsrechtslage entsprochen (Art. 6 Abs. 1 der Landesverfassung).

10. Forschung

Was bereits im I. Tätigkeitsbericht (S. 55) als Tendenz angesprochen wurde, hat sich auch im Berichtszeitraum fortgesetzt. In zunehmender Zahl wurden dem Landesbeauftragten Konzepte für anstehende Forschungsvorhaben zur datenschutzrechtlichen Überprüfung bzw. Beratung zugeleitet. Dabei wurde deutlich, daß bezüglich der gesetzlichen Anforderungen an die Zulässigkeit einer solchen Datenerhebung noch Informationsbedarf besteht, auch wenn die Forscher die allgemeinen gesetzlichen Grundlagen erkannt und berücksichtigt haben. Häufig fehlte auch das Wissen um die gesetzlich in § 4 Abs. 2 DSG-LSA vorgeschriebene Form einer wirksamen Einwilligung der Betroffenen.

Im Gegensatz zur normalen Einwilligung, in der lediglich die Zustimmung abverlangt wird, schreibt das DSG-LSA die **informierte Einwilligung** vor. Das heißt, daß der Betroffene über die Bedeutung der Einwilligung, den Zweck der Speicherung, einer vorgesehenen Übermittlung, die Art der Daten und die Form der Verarbeitung vorab zu informieren ist. Des weiteren gehört dazu der Hinweis auf die Rechte des Betroffenen, z.B. die Möglichkeit der Verweigerung der Einwilligung und deren Folgen für den Betroffenen und die Widerrufsmöglichkeit für die Zukunft. Damit die vorgenannten Informationen den Betroffenen auch erreichen, schreibt das Gesetz auch die äußere Form der Einwilligung vor. So ist die Einwilligungserklärung - von besonderen Ausnahmen abgesehen - schriftlich zu erteilen und, wenn sie sich innerhalb anderer Informationen versteckt, im äußeren Erscheinungsbild hervorzuheben.

Die folgenden Beispielsfälle sollen einen Überblick über die Vielfalt der Probleme geben.

10.1 Ursachen rechtsextremistischer Gewalt bei Jugendlichen und Heranwachsenden in den neuen Bundesländern

Das Ministerium der Justiz erteilte zwei führenden Kriminologen den Auftrag zur wissenschaftlichen Untersuchung der Ursachen rechtsextremistischer Gewalt bei Jugendlichen und Heranwachsenden in den neuen Bundesländern, um das in dem bisherigen Ausmaß nicht bekannte Phänomen, das gleichzeitig von hoher politischer Brisanz und Aktualität ist, konkret zu beleuchten.

Das Konzept sah eine Aktenauswertung von Strafverfahren gegen rechtsextremistische Gewalttäter sowie eine Befragung inhaftierter Gefangener vor. Die Datenerhebung beruhte auf der freiwilligen Teilnahme, und es war vorgesehen, die Einwilligung bei den Betroffenen einzuholen. Diese Verfahrensweise entsprach den Bestimmungen des DSG-LSA.

Der Landesbeauftragte wies aber auf folgendes hin:
Bei der Einwilligungserklärung ist die Handlungsfähigkeit der Betroffenen zu beachten. Für den Fall, daß diese bei Jugendlichen nicht vorliegt, ist die Einwilligung der gesetzlichen Vertreter erforderlich. Fragen nach der familiären

Situation und der Biographie der Herkunftsfamilie können u.U. in die Rechte Dritter eingreifen. Der Schutz Dritter muß jedoch zwingend gewährleistet sein.

Die datenschutzrechtlichen Hinweise des Landesbeauftragten wurden in das Konzept eingearbeitet.

10.2 Nachbeobachtung der Teilnehmer an einer Gerontologischen Studie

In den Jahren 1983 bis 1985 wurden hier Vorruheständler auf ihren körperlichen und psychophysischen Funktionszustand hin untersucht. Erhoben wurden dabei Merkmale zum Beruf, zur Berufszufriedenheit, zur sozialen Lage und zur sozialen Kompetenz.
Ziel des jetzigen neuen Forschungsprojektes ist es, nach Ablauf von nunmehr 10 Jahren, Aussagen zum relativen Beitrag summarischer, sozialer, arbeitsbedingter und psychologischer Merkmale für die genannten Endpunkte und Hinweise auf Merkmale, die im Rahmen eines geriatrischen Screenings prognostisch relevant sind (Funktion, Hilfebedarf, Unterstützung) zu erhalten.

Bei dieser Studie war zu berücksichtigen, daß die Ausgangsdaten 1983 bis 1985 nach dem Recht der ehemaligen DDR ohne Einwilligung erhoben worden waren, die jetzt beabsichtigten Nacherhebungen aber im Rahmen des heute geltenden Rechts erfolgen müssen. Deshalb war vorgesehen, die Daten von Probanden, die nicht einwilligen, verstorben oder unbekannt verzogen waren, zu anonymisieren.

Die im Konzept dargestellte Vorgehensweise entspricht weitestgehend den heutigen gesetzlichen Bestimmungen. Die Probanden sollen ihre Einwilligung zur Nachbeobachtung erteilen sowie in die Nutzung der bisher gespeicherten Angaben einwilligen. Aufgrund der besonderen Situation (Erhebung der Ausgangsdaten nach dem Recht der ehemaligen DDR ohne Einwilligung der Betroffenen) hat der Landesbeauftragte darauf hingewiesen, daß das Anonymisieren der Daten von Betroffenen, die heute ihre Einwilligung verweigern, nicht ausreicht.
Gemäß § 16 Abs. 2 DSG-LSA sind deren personenbezogene Daten zu löschen, weil ihre (weitere) Speicherung unzulässig ist.

Die Hinweise des Landesbeauftragten wurden in der endgültigen Konzeption berücksichtigt.

10.3 Kerndokumentation Rheuma

Gemeinsam mit 21 anderen Rheumazentren und dem Deutschen Forschungszentrum Berlin wird an einem öffentlichen Krankenhaus in Sachsen-Anhalt die Versorgungssituation von Rheumakranken untersucht. Ziel ist es, eventuelle Lücken zu erkennen und notwendige Konsequenzen zur Schließung der Lücken in die Wege zu leiten.

Im Rahmen dieser Studie wurden dem Landesbeauftragten vom Krankenhaus die verwendeten Fragebögen übersandt mit dem Hinweis, es handele sich nach dortiger Auffassung nicht um personenbezogene, sondern anonymisierte Daten.

Der Landesbeauftragte teilte die Auffassung des Krankenhauses nicht, da im Patientenfragebogen Angaben abgefordert wurden, die insgesamt Rückschlüsse auf bestimmte oder bestimmbare Personen zulassen (z.B. Geschlecht, Familienstand, Gemeinde mit Postleitzahl, Großstädte mit Stadtteilen). Damit gelten die Schutzvorschriften des DSG-LSA.
Das Krankenhaus wurde darauf hingewiesen, daß datenschutzrechtliche Bedenken nur dann zurückgestellt werden können, wenn auf die Angaben "Gemeinde mit Postleitzahl bzw. bei Großstädten die Stadtteile" verzichtet wird und die Zuordnung lediglich zum Kreis/Stadt abgefragt wird. Durch diese Zuordnung ist ein Rückschluß auf eine bestimmte bzw. bestimmbare Person nicht mehr möglich.
Das Krankenhaus folgte diesen Hinweisen.

10.4 "Mainzer Modell" und "Magdeburger Fehlbildungsregister"

Der Landesbeauftragte erhielt davon Kenntnis, daß die Otto-von-Guericke-Universität ein in Mainz (in den Jahren 1989 bis 1992) durch das Bundesministerium für Gesundheit gefördertes Modell "Einrichtung eines Erfassungsprogramms für angeborene Fehlbildungen bei Neugeborenen" auf Praktikabilität der

Erfassung nach den Kriterien des in Mainz standardisierten Handbuches erprobt. Der Erprobungszeitraum soll sich auf den Zeitraum von 01.07.1992 bis 30.06.1995 erstrecken.

Eine Sichtung der in Mainz verwendeten Projektunterlagen ergab, daß dort keine Datenerhebung beim Patienten erfolgt, sondern anonymisierte Daten den Patientenakten sowie vorhandenen Aufzeichnungen (Befunden) entnommen werden.

Ganz anders präsentierten sich die in Magdeburg verwendeten Fragebögen. Die Forscher hatten die Bögen des "Mainzer Modells" mit eigenen Fragebögen des "Magdeburger Fehlbildungsregisters" unter der Bezeichnung "EUROCAT - Registration angeborener Anomalien" erweitert. Anstelle der vorgesehenen Entnahme anonymisierter Daten wurde eine direkte Erhebung personenbezogener Daten vorgenommen. So wurden beispielsweise bei der Mutter nicht nur Daten zur eigenen Person, sondern auch zur Person des Vaters und des Kindes erhoben. Diese Befragungen wurden außerdem nicht auf Neugeborene mit Fehlbildungen beschränkt, sondern generell bei allen Neugeborenen durchgeführt. Die Fragebögen des "Mainzer Modells" wurden hierzu inhaltlich verändert.

Der Landesbeauftragte hat deshalb gebeten, die Durchführung des Forschungsvorhabens in dieser Form sofort zu ändern bzw. einzustellen, weil damit massiv gegen das informationelle Selbstbestimmungsrecht der Betroffenen verstoßen wird, weil zum einen die Aufnahme **aller** Neugeborenen in das Fehlbildungsregister vom Forschungsauftrag nicht gedeckt ist und im übrigen die bei den Fragebögen vorgesehene Einwilligungserklärung der Mutter nicht der in § 4 Abs. 2 DSG-LSA vorgeschriebenen Form entspricht.

Auch bei einer (ausreichenden) Einwilligung der Mutter konnte nicht auf die Einwilligung des Vaters verzichtet werden; zum einen für Angaben zu seiner Person, aber auch zu den Angaben des Kindes.

Die Otto-von-Guericke-Universität hat dazu schriftlich erklärt, sie habe die Durchführung des bisherigen Projektes im September 1994 eingestellt.

Inzwischen hat die Universität ihre Verfahrensweise zur Überprüfung des „Mainzer Modells“ umgestellt und an den Forschungsauftrag angepaßt.

Zum "Magdeburger Fehlbildungsregister" ist vor Wiederaufnahme des Projektes ein Konzept zu erarbeiten und einer datenschutzrechtlichen Überprüfung zu unterziehen. Dabei ist das Ministerium für Arbeit, Soziales und Gesundheit als verantwortliche oberste Landesbehörde nach § 14 Abs. 1 DSG-LSA gefordert. Die bisherige Fachaufsicht entsprach dem nicht immer.

10.5 Sozialhilfedynamik in den neuen Bundesländern

Bei dem o.a. Forschungsprojekt handelt es sich um eine Studie zum Verlauf der Sozialhilfe. Die Forschungsgruppe hatte vorgesehen, das Forschungsprojekt in zwei Stufen durch eine Befragung von Sozialhilfeempfängern und eine Aktenauswertung beim Sozialamt durchzuführen.

Der Landesbeauftragte hat in seiner Stellungnahme darauf hingewiesen, daß es sich bei dem Forschungsprojekt um die Verarbeitung von Sozialdaten handelt, deren Offenbarung nur unter den Voraussetzungen der §§ 67 bis 77 SGB X (a.F.) zulässig ist. Eine Voraussetzung für die Übermittlung von Daten wäre die vorherige Genehmigung der zuständigen obersten Landesbehörde, mithin durch das Ministerium für Arbeit, Soziales und Gesundheit. Einer Genehmigung bedarf es jedoch nicht, soweit es zumutbar ist, die Einwilligung des Betroffenen einzuholen.

Zur Befragung der Sozialhilfeempfänger hatte die Forschergruppe vorgesehen, den Kontakt mit den Betroffenen über das Sozialamt im Wege der Adressenvermittlung aufzunehmen. Dazu wurden dem Sozialamt kuvertierte Schreiben an die Betroffenen zur Verfügung gestellt, die von dort adressiert und postalisch versendet wurden. Im Falle der Bereitschaft zur Teilnahme an dem Forschungsprojekt konnte der Adressat die Verbindung zur Forschungsgruppe selbst aufnehmen.

Datenschutzrechtlich ist diese Form der Kontaktaufnahme eine gute Lösung, die die schutzwürdigen Belange der Betroffenen berücksichtigt. Ergänzend hat der Landesbeauftragte vorgeschlagen, bei der Kontaktaufnahme die Einwilligung zur Teilnahme an dem Forschungsprojekt schriftlich einzuholen.

In einem zweiten Schritt war beabsichtigt, per Zufallsauswahl Sozialhilfeakten auszuwerten. Hierzu war vorgesehen, durch die Forscher eine Grobauswertung der Akten ohne Einwilligung der Betroffenen nach dem Zufallsprinzip vorzunehmen. Begründet wurde der Schritt damit, daß es aus organisatorischen und inhaltlichen Gründen nicht zumutbar sei, die Einwilligung der Betroffenen einzuholen.
Der Landesbeauftragte hat dazu auf die gesetzliche Regelung des § 75 Abs. 1 SGB X hingewiesen, wonach von gesetzlich vorgesehenen Einwilligungen des Betroffenen nur ausnahmsweise abgewichen werden darf. Das könnte dann der Fall sein, wenn es unzumutbar ist, den Zweck der Forschung oder Planung auf andere Weise zu erreichen. Diese Anforderungen sind im Interesse der Persönlichkeitsrechte der Betroffenen eng auszulegen. Die von der Forschungsgruppe angeführten organisatorischen Gründe reichten dafür nicht aus.

Den Anregungen des Landesbeauftragten ist die Forschungsgruppe gefolgt. Für den zweiten Schritt wurde das Konzept dahingehend verändert, daß die Daten bei den Betroffenen durch Mitarbeiter des Sozialamtes erhoben und anonymisiert an die Forschergruppe übermittelt werden.

10.6 Errichtung klinischer Tumorregister

Am Städtischen Klinikum Dessau, an der Medizinischen Fakultät der Martin-Luther-Universität Halle-Wittenberg und an der Medizinischen Fakultät der Otto-von-Guericke-Universität Magdeburg wurden klinische Tumorregister eingerichtet bzw. befinden sich solche klinischen Tumorregister im Aufbau. Ziel dieser Tumorregister ist u.a., in den kommenden Jahren eine gleichmäßige Verbesserung der Versorgung Krebskranker zu erreichen sowie die strukturierten Formen fachübergreifender Zusammenarbeit des medizinischen Wissens über die Krebsbehandlung zu bündeln.

Die datenschutzrechtliche Überprüfung der übersandten Konzepte für die Tumorregister ergab, daß das DSG-LSA auf die Register nicht anzuwenden ist, weil sie in der Rechtsform eines eingetragenen Vereins geführt werden und als solche weder nach ihrer rechtlichen Form noch nach ihrer inneren Struktur (Mitgliedschaft) öffentliche Stellen im Sinne des § 3 DSG-LSA sind. Für die automatisierte **Führung des Tumorregisters** gelten deshalb die Bestimmungen des BDSG für nicht-öffentliche Stellen.

Da aber ausweislich der Vereinssatzungen u.a. auch Ärzte aus **staatlichen** Krankenhäusern ordentliche Mitglieder des Vereins werden können, hat der Landesbeauftragte vorsorglich darauf hingewiesen, daß diese Mitglieder bei der **Übermittlung** personenbezogener Daten von Krankenhauspatienten an die Tumorregister die engen Grenzen des DSG-LSA zu beachten haben.

Jede Form der personenbezogenen Datenverarbeitung (dazu gehört auch die Datenübermittlung) in oder aus staatlichen Einrichtungen (z.B. Krankenhäusern) unterliegt der Kontrolle des Landesbeauftragten.

11. Gesundheitswesen

11.1 Krankenversicherungskarte

Durch das Gesundheits-Reformgesetz vom 20.12.1988 (BGBl. I S. 2477) hat der Gesetzgeber festgelegt, daß der bisher in der gesetzlichen Krankenversicherung verwandte Krankenschein durch die Krankenversicherungskarte ersetzt werden soll, die dem Arzt bei Behandlungsbeginn vom Versicherten vorzulegen ist (§ 291 Abs. 1 SGB V). Neben der Unterschrift des Versicherten darf die Krankenversicherungskarte nach § 291 Abs. 2 SGB V ausschließlich folgende Daten enthalten:

1. Bezeichnung der ausstellenden Krankenkasse,
2. Familienname und Vorname des Versicherten,
3. Geburtsdatum,
4. Anschrift,
5. Krankenversicherungsnummer,

6. Versichertenstatus,
7. Tag des Beginns des Versicherungsschutzes,
8. bei befristeter Gültigkeit der Karte das Datum des Fristablaufs.

Mit Ausnahme des Geburtsdatums und der Anschrift sind alle genannten Daten auf der Karte im Klartext aufgedruckt. Die Aufnahme weiterer Patientendaten in die Karte oder die Steuerung, Überwachung oder Kontrolle medizinischer Leistungen über die Karte ist nicht erlaubt. Änderungen oder Ergänzungen des Karteninhaltes sind ohne neue gesetzliche Bestimmungen nicht zulässig.

Die zuständigen Spitzenverbände der Krankenkassen und die Kassenärztliche Bundesvereinigung regelten vertraglich die Einzelheiten über die bundesweite Einführung und entschieden sich für eine Chipkarte. Aus datenschutzrechtlicher Sicht bietet die Chipkartentechnologie grundsätzlich umfassendere Möglichkeiten zur Datensicherung als z.B. eine Magnetstreifenkarte, da die Chipkarten mit Paßwörtern u.ä. die Zugriffsberechtigungen sichern, während die Magnetstreifenkarten grundsätzlich lesbare Daten enthalten und nicht durch einen in das Medium integrierten Zugriffsschutz gesichert werden können.
Die Datenschutzbeauftragten der Länder und des Bundes werden im Rahmen ihrer Kontrolltätigkeit auch überprüfen, ob nur die gesetzlich zugelassenen Daten auf den Chipkarten gespeichert sind und ob die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

In ihrer 47. Konferenz haben die Datenschutzbeauftragten des Bundes und der Länder am 10.03.1994 auch einen Beschluß zur Verwendung von Chipkarten im Gesundheitswesen gefaßt **(Anlage 5).**

Der Landesbeauftragte sieht die in der Planung befindlichen neuen Karten, wie z.B. die BKK-Gesundheits-Card (BKK-Card), DiagnostiX-Card, Röntgen-Card, „VitalCARD“, Patienten-Chipkarten der Apotheke (A-Card), als langfristig gefährliche Verstrickung des einzelnen Betroffenen in eine Informations- und Technikabhängigkeit, die sein Recht auf selbstbestimmte Entscheidungen im für ihn so wichtigen medizinischen Bereich immer mehr einzuschränken droht.

11.2 Datenschutz in Posteingangsstellen der Krankenhäuser und Gesundheitsämter

In allen Behörden gibt es zentrale Posteingangsstellen, die regelmäßig so arbeiten, daß dort die gesamte ein- und ausgehende Post entgegengenommen bzw. abgefertigt wird. Die eingehende Post wird fast ausnahmslos geöffnet, was in einem Massenbetrieb zur Gewährleistung eines raschen und ungehinderten Durchlaufs auch unumgänglich ist. Lediglich persönlich adressierte **und** als solche identifizierbare Privatpost bleibt ungeöffnet.

Diese Verfahrensweise kann im Hinblick auf die sensitiven Eingänge in Krankenhäusern und Gesundheitsämtern nicht uneingeschränkt angewendet werden. Vielmehr folgt aus dem auch gesetzlich besonders geschützten persönlichen Vertrauensverhältnis zwischen Arzt und Patient die Pflicht der Verwaltungen, eingehende Arztpost anders zu behandeln als die üblichen Verwaltungseingänge.

Das Patientengeheimnis ist seit alters her im Standesrecht der Ärzte verankert. Seine Einhaltung ist darüber hinaus auch strafrechtlich in § 203 StGB geschützt. Sendungen, die an einen Arzt adressiert sind oder erkennbar medizinischen Inhalt haben, sind deshalb ungeöffnet diesem zuzuleiten. Nur so ist gewährleistet, daß das Vertrauen, das der Patient in seinen Arzt setzt, bestmöglich geschützt ist und Informationen, die der Patient seinem Arzt zukommen lassen will, diesen auch unmittelbar erreichen. Da vom Arztgeheimnis gem. § 203 Abs. 3 StGB auch sog. Hilfspersonen erfaßt sind, zählen auch die unmittelbaren Mitarbeiter des Arztes zum öffnungsberechtigten Personenkreis.

11.3 Richtlinien für die Einführung neuer Untersuchungs- und Behandlungsmethoden (NUB-Richtlinien)

Aufgrund der § 92 Abs. 1 Ziff. 5 SGB V i.V. mit §135 SGB V sollen die Bundesverbände der Ärzte und Krankenkassen Richtlinien über die Einführung neuer Untersuchungs- und Behandlungsmethoden beschließen. Von dieser Ermächtigung haben die genannten Bundesverbände am 04.12.1990 Gebrauch gemacht und die Richtlinien zur Methadonsubstitutionsbehandlung bei intravenös Heroinabhängigen erlassen.

Diese Richtlinien wurden am 16.02.1994 modifiziert und waren aufgrund ihrer bundesweiten Auswirkung Gegenstand mehrerer Besprechungen in den Arbeitskreisen der Datenschutzbeauftragten, weil die Wahrnehmung des informationellen Selbstbestimmungsrechts und der Schutz des in die Behandlung einbezogenen Patienten auch dann gewährleistet sein muß, wenn er sich aufgrund seiner gesundheitlichen Verfassung ggf. zu einer bedingungslosen Zusammenarbeit mit der ihn behandelnden Einrichtung bereit erklärt.

Die Kassenärztliche Vereinigung Sachsen-Anhalt trat in diesem Zusammenhang Anfang 1994 mit der Bitte um datenschutzrechtliche Beratung an den Landesbeauftragten heran. Das Kernproblem war die Anonymisierung der personenbezogenen Daten der zu Substituierenden zum frühestmöglichen Zeitpunkt. Nach übereinstimmender Meinung der Beteiligten soll diese Anonymisierung spätestens bei der Geschäftsstelle der Methadonkommission einsetzen. Die Mitglieder der Kommission entscheiden dann nur über einen anonymisierten Fall.

Die Gespräche mit der Kassenärztlichen Vereinigung sind abgeschlossen; die Anregungen des Landesbeauftragten wurden berücksichtigt, so daß nur der behandelnde Arzt und die abrechnende Krankenkasse die personenbezogenen Daten im Einzelfall kennen.

11.4 Notarzteinsatzprotokoll und Rettungsdienst

Ein Arzt eines Krankenhauses wandte sich an den Landesbeauftragten mit der Bitte um Überprüfung, ob die Anweisung des Verwaltungsdirektors rechtens sei, die Notarzteinsatzprotokolle, die eine Fülle personenbezogener und medizinischer Daten enthalten, an den Träger des Rettungsdienstes bzw. dessen Leistungserbringer für Abrechnungszwecke auszuhändigen.

Die Beantwortung dieser Anfrage ergibt sich nunmehr unmittelbar aus dem Rettungsdienstgesetz des Landes Sachsen-Anhalt vom 11.11.1993 (GVBl. LSA S. 699), das als sog. bereichsspezifische Regelung seit dem 16.12.1993 anzuwenden ist. Nach § 23 Abs. 1 RettDG-LSA dürfen personenbezogene Daten nur erhoben, gespeichert oder genutzt werden, soweit dies erforderlich ist für

1. die Durchführung eines Einsatzes,
2. die unmittelbare Versorgung eines Patienten,
3. die Abwicklung eines Beförderungsauftrages, insbesondere die Abrechnung der erbrachten Leistung.

Im übrigen gelten - auch für die Übermittlung personenbezogener Daten - die Bestimmungen des DSG-LSA (§ 23 Abs. 2 RettDG-LSA). Daraus ergibt sich, daß das Gesetz für diese Abrechnungszwecke eine Übermittlung medizinischer Daten des Patienten nicht vorsieht. Dem Leistungserbringer können nur die sog. Stammdaten (Name, Vorname, Geburtsdatum, Anschrift, Krankenkasse, Ort und Zeitpunkt des Einsatzes) zugänglich gemacht werden.

Daher war die Anweisung des Verwaltungsdirektors an den Arzt, medizinische Daten ohne Einverständniserklärung des Patienten an einen Dritten zu übermitteln, rechtswidrig.
Auch vor Inkrafttreten des Rettungsdienstgesetzes war die Datenübermittlung nach den damals direkt geltenden Bestimmungen des DSG-LSA unzulässig.

Nach eingehender Information über die Rechtslage hat im vorliegenden Fall sowohl das Krankenhaus als auch der Landkreis als Träger des Rettungsdienstes die Übermittlung der medizinischen und der anderen nicht erforderlichen personenbezogenen Daten an den Rettungsdienst abgestellt.

Der Fall war für den Landesbeauftragten Anlaß, den Umgang mit den personenbezogenen Daten der Betroffenen durch die Rettungsdienste im Land stichprobenweise zu überprüfen. Die daraus resultierenden Erkenntnisse wurden mit dem Ministerium für Arbeit, Soziales und Gesundheit und im Landesbeirat für das Rettungswesen erörtert. Das Ministerium hat anschließend nach Beratung durch den Landesbeauftragten durch Erlaß vom 9. Januar 1995 (MBl. LSA

S. 174) den Inhalt und die Verteilung der Notarztprotokolle datenschutzgerecht geregelt.
Eine entsprechende Regelung ist in Kürze für die Rettungseinsätze ohne Notarzt zu erwarten.

12. Gewerbe, Handwerk und Wirtschaft

12.1 Architektengesetz

Im Land Sachsen-Anhalt gilt zur Zeit noch das Gesetz zum Schutz der Berufsbezeichnung Architekt und zur Vorbereitung der Errichtung von Architektenkammern in den künftigen Ländern der Deutschen Demokratischen Republik
- Architektengesetz - vom 19. Juli 1990 und die dazu ergangene Ordnung über die Aufgaben und Arbeitsweise der Architektenkammern. Dieses nunmehr überholte Recht soll durch ein neues Architektengesetz novelliert werden.
Seitens der Landesregierung wurde der Landesbeauftragte schon beim Entwurf beteiligt. Aufgrund seiner Anregungen wurden verschiedene datenschutzrelevante Regelungen mit aufgenommen, wie z.B. Kriterien für die Datenlöschung aus dem Verzeichnis der auswärtigen Architekten/Stadtplaner und konkrete Bestimmungen zur Auskunftspflicht.

Der Gesetzentwurf wird voraussichtlich im 1. Halbjahr 1995 in den Landtag eingebracht.

12.2 Novellierung der Handwerksordnung

Im (Bundes-)Gesetz zur Änderung der Handwerksordnung, anderer handwerksrechtlicher Vorschriften und des Berufsbildungsgesetzes vom 20.12.1993 ist im Datenkatalog der Anlage D für die Lehrlingsrolle die Aufnahme der Adresse des Lehrlings unterblieben, die Aufnahme der Anschrift seines gesetzlichen Vertreters aber erfolgt.

Der Landesbeauftragte hat unter diesen besonderen Umständen gegen die übergangsweise ohne gesetzliche Grundlage vorgenommene Speicherung der Anschrift des Lehrlings dann keine datenschutzrechtlichen Bedenken, wenn in absehbarer Zeit der Fehler durch eine Novellierung der Handwerksordnung behoben wird.

Nach Aussagen des Ministeriums für Wirtschaft und Technologie des Landes Sachsen-Anhalt ist auf Arbeitsebene beabsichtigt, zu Beginn der Legislaturperiode des Bundestages die entsprechende Korrektur der Anlage zu veranlassen.

12.3 Änderung der Gewerbeordnung

Mit dem Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 23. November 1994 wurde die Gewerbeordnung um Datenschutzregelungen erweitert. Der neu eingefügte § 11 regelt die Erhebung, Verarbeitung und Nutzung personenbezogener Daten. Darin wird in Absatz 1 auch zugelassen, daß Daten aus bereits abgeschlossenen oder sonst anhängigen Verfahren (gewerberechtliche Verfahren, Straf- oder Bußgeldverfahren, Vergleichs- oder Konkursverfahren, versicherungsrelevante Verfahren, arbeitserlaubnisrechtliche Verfahren) erhoben werden dürfen. Außerdem verweist Absatz 6 für das Verändern, Sperren oder Löschen der erhobenen Daten auf die Datenschutzgesetze der Länder.
Die Änderungen in § 14 legitimieren bei der Gewerbeanzeige die Erhebung und Verarbeitung von Daten. Wesentlich ist die vorgenommene Festlegung der Zweckbindung. Neu geregelt wurde auch - sowohl für Auskunftsverlangen öffentlicher wie nicht-öffentlicher Stellen - die Übermittlung von Daten aus der Gewerbeanzeige. Bei Nachweis des berechtigten Interesses dürfen der Name, die betriebliche Anschrift und die angezeigte Tätigkeit des Gewerbetreibenden übermittelt werden.

Damit wurde einem alten Anliegen der Datenschutzbeauftragten und einem großen Problem in der täglichen Verwaltungspraxis endlich zufriedenstellend abgeholfen. Hierzu hatte es in der Vergangenheit beim Landesbeauftragten immer wieder Anfragen gegeben.

12.4 Datenübermittlung bei der Industrie- und Handelskammer

Im Rahmen eines Erfahrungsaustausches zwischen den Datenschutzbeauftragten der Länder wurde die Mitteilung von Prüfungsergebnissen an Ausbildungsbetriebe durch die Industrie- und Handelskammern überprüft.

Der Landesbeauftragte stellte fest, daß in Sachsen-Anhalt Prüfungsergebnisse von Abschlußprüfungen nur insoweit dem Ausbildenden übermittelt werden, wie dies in § 23 der "Prüfungsordnung für die Durchführung von Prüfungen in anerkannten Ausbildungsberufen" zugelassen ist.
Somit erhält der Ausbildende nur dann einen schriftlichen Bescheid über die Prüfung, wenn die Prüfung nicht bestanden wurde. Darüber hinaus werden keine Prüfungsergebnisse weitergegeben.

Der Landesbeauftragte sieht bei einer solchen Verfahrensweise keine datenschutzrechtlichen Bedenken.

12.5 Ehemalige Mitarbeiter des MfS bei Detekteien und privaten Sicherheitsdiensten

Zu einer Eingabe an den Petitionsausschuß des Landtages wurde der Landesbeauftragte vom Ministerium für Wirtschaft und Technologie um Stellungnahme gebeten. Der Petent sah "mögliche Gefahren durch ehemalige Mitarbeiter des MfS" als Beschäftigte in Detekteien und privaten Sicherheitsdiensten und hatte sich deshalb an den Deutschen Bundestag und den Landtag von Sachsen-Anhalt gewandt.

Der Landesbeauftragte wies im Rahmen seiner Zuständigkeit für die **öffentlichen** Stellen des Landes darauf hin, daß der in § 14 Abs. 1 DSG-LSA normierte Grundsatz der Verantwortlichkeit für effektiven Datenschutz auch die Pflicht umfaßt, im öffentlichen Bereich für Bewachungsaufgaben nur zuverlässige und überprüfte private Personen und Betriebe einzusetzen.

Eine öffentliche Stelle, die sich von Dritten bewachen läßt, muß außerdem nach § 6 DSG-LSA durch technische und organisatorische Maßnahmen sicherstellen, daß die Bewacher Datenverarbeitungsanlagen und Datenträger jeder Art in der Behörde nicht unbefugt erreichen oder benutzen können.

Zusätzlichen strafrechtlichen Schutz gibt neben den allgemeinen Tatbeständen des Strafgesetzbuches als spezielle Strafvorschrift § 31 DSG-LSA.
Neue bereichsspezifische Datenschutzregelungen zur besseren Überprüfung der Beschäftigten im Bewachungsgewerbe finden sich jetzt in dem Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften vom 23.11.1994 (BGBl. I S. 3475).

12.6 Standort- und Liegenschaftsinformationssystem (SOLIS-G)

Erst aus der Antwort der Landesregierung auf die Kleine Anfrage eines Landtagsabgeordneten wurde dem Landesbeauftragten die Existenz eines Standort- und Liegenschaftsinformationssystems bekannt. Er bat daraufhin das zuständige Ministerium für Wirtschaft und Technologie um Mitteilung, welche Daten im Rahmen des Systems gespeichert werden, und wies auf die gesetzlichen Verpflichtungen des DSG-LSA hin.
Aus den vom Ministerium zur Verfügung gestellten Unterlagen ergab sich, daß die in dem Informationssystem gespeicherten Daten in der Regel nicht personenbezogen sind bzw. juristische Personen betreffen, die vom DSG-LSA nicht geschützt werden. SOLIS-G enthält zur Verbesserung der touristischen und gewerblichen Infrastruktur Standortdaten der für potentielle Erwerber zur Verfügung stehenden Liegenschaften.

Sofern es sich bei den gespeicherten Grundstückseigentümern, den Planungsträgern und den Firmen, die sich bereits in den entsprechenden Gebieten angesiedelt haben, ausnahmsweise um natürliche Personen handelt, muß im Einzelfall die Zulässigkeit der Übermittlung dieser Daten nach § 12 Abs. 1 Ziff. 2 DSG-LSA geprüft werden. Im allgemeinen wird bei den Empfängern des Informationsmaterials jedoch ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten vorliegen und bei den Betroffenen kein schutzwürdiges Interesse am

Ausschluß einer Übermittlung bestehen. Vielmehr gibt es im Regelfall ein wirtschaftliches Eigeninteresse an der Übermittlung der Daten.

Der Landesbeauftragte hat daher keine grundsätzlichen datenschutzrechtlichen Bedenken gegen das gewählte Informationssystem.

13. Hinweise zum technischen und organisatorischen Datenschutz

13.1 Kontrolle des technischen und organisatorischen Datenschutzes

Durch den Landesbeauftragten wurden im Berichtszeitraum nach § 22 Abs. 1 DSG-LSA in den Polizeidirektionen und Polizeiinspektionen des Landes, den Staatsanwaltschaften sowie in einer Reihe von Einwohnermeldeämtern, Straßenverkehrsämtern und bei Verwaltungsgemeinschaften auch Kontrollen der technischen und organisatorischen Datensicherheit durchgeführt.
Grundlage für die Überprüfung der technischen und organisatorischen Maßnahmen bildet § 6 DSG-LSA. Er verpflichtet alle öffentlichen Stellen, diejenigen technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um weitestgehenden Schutz für die personenbezogenen Daten während deren Aufbewahrung und beim Umgang mit ihnen zu gewährleisten.
So ist es z.B. nicht beliebig zulässig, einmal vom Bürger bereits erhaltene Daten erneut anzufordern. Wer als öffentliche Stelle ihm anvertraute personenbezogene Daten unzureichend gesichert automatisiert verarbeitet, riskiert, auch ohne Verschulden, hohe Schadenersatzleistungen, wenn dem betroffenen Bürger dadurch ein Schaden entsteht (§ 18 DSG-LSA).
Es gehört deshalb zur Kontrollpraxis, bei der Überprüfung von Sicherungsmaßnahmen auch besondere Risikofaktoren, wie z.B. Einbruch, Sabotage, Brand, Wasser, Gas und Blitzschlag, mit Hinweisen zu berücksichtigen. So erfordert der Einsatz elektrischer/elektronischer Geräte (Arbeitsplatz-PC, Zentralrechner u.ä.) bei der automatisierten Datenverarbeitung stets auch die sofortige Verfügbarkeit geeigneter Löschtechnik für eventuell auftretende Brände, um den Erhalt des gespeicherten Datenbestandes zu gewährleisten sowie möglichen immateriellen Schaden zu minimieren.

13.1.1 Defizite bei der Datensicherheit

Besondere Bedeutung kommt dabei für die automatisierte Datenverarbeitung den in § 6 Abs. 2 DSG-LSA enthaltenen sog. "**10 Geboten** des technischen und organisatorischen Datenschutzes“ zu.

Defizite bei der Zugangskontrolle und der sicheren Aufbewahrung von Datenträgern, auf die der Landesbeauftragte bereits im I. Tätigkeitsbericht hingewiesen hat (S. 71), stehen wieder ganz oben auf der Mängelliste.
Behördenübergreifend waren typische Mängel:

- unsichere Zugangstüren (mit z.B. abschraubbaren Türschloßblenden, herausragenden Schließzylindern, Oberlichtern im Türblatt, blechverkleidete "Papptüren“, einfache Türzargen ohne Mehrfachverriegelungsfunktion, mit Einbausicherungen nachgerüstete Türschlösser ohne Nachweis oder Kenntnis der Anzahl der Ersatzschlüssel),
- unsichere Fenster, z.B. mit Einfachverglasung, ohne ausreichenden Sichtschutz bei parterre gelegenen Räumen, defekte Rolläden, nicht verschließbare Fensterriegel,
- fehlende oder ungeeignete Feuerlöscher für die Bekämpfung von Bränden in elektrischen Anlagen,
- Zugriffsmöglichkeiten auf personenbezogene Daten in EDV-Anlagen (hauptsächlich bei Einzelplatz-PC) ohne Paßwortabfrage, keine Sicherheitssoftware,
- kein oder nur ein ungenügendes Backup-Verfahren, ungenügende oder fehlende Prüfung der Reproduzierbarkeit gesicherter Datenbestände,
- unsachgemäße und nicht sicher aufbewahrte Backup-Datenträger (z.B. in Schreibtischschubladen, in Regalen, in nicht feuersicheren Blechschränken),
- fehlende oder unvollständige Dateifestlegungen, Dateienregistermeldungen oder Geräteverzeichnisse.

Die Entsorgung von Altakten mit personenbezogenen Daten wurde nicht selten der Müllabfuhr überlassen. Aktenvernichter oder Verträge mit Aktenvernichtungsunternehmen bildeten die Ausnahme.

Verschiedentlich wurden Karteikartensammlungen oder Akten vorgefunden, auf denen die Personenkennzahl der Bürger noch vermerkt war, obwohl deren weitere Speicherung nach dem Einigungsvertrag längst unzulässig ist.

13.1.2 Versäumnisse bei der Zugangskontrolle

Anlaß für besondere Kontrollen waren sich häufende Einbruchsdiebstähle bei öffentlichen Stellen der Landes- und auch der Kommunalverwaltung. In vielen Fällen waren Versäumnisse im Bereich des Zugangsschutzes mit ursächlich.
Zwar ging es den Tätern meist um die Beschaffung neuwertiger Hardware und nicht um eine gezielte Beschaffung personenbezogener Daten. Bei einigen Einbrüchen war aber dabei mittelbar auch der Verlust gespeicherter personenbezogener Datenbestände zu verzeichnen. Bewährt hat sich als Vorsorgemaßnahme die verschlüsselte Ablage der Daten auf der Festplatte, weil damit die Mißbrauchsgefahr entfällt. Auch eine ordnungsgemäße Datensicherung (Sicherungskopien) relativiert den immateriellen Schaden.

Diese Ereignisse veranlassen den Landesbeauftragten, auf die Informationsmöglichkeit bei den kriminalpolizeilichen Beratungsstellen hinzuweisen. Diese sollten auch von öffentlichen Stellen des Landes bei der Vorbereitung von Baumaßnahmen für zentrale Räume mit Informationstechnik in Anspruch genommen werden.

13.2 Auftragsdatenverarbeitung

Die Bedingungen zur Vergabe von Aufträgen zur Verarbeitung personenbezogener Daten durch öffentliche Stellen des Landes Sachsen-Anhalt als Auftraggeber an öffentliche oder nicht-öffentliche Stellen als Auftragnehmer und die dabei entstehenden Rechtsverhältnisse sind in § 8 DSG-LSA geregelt. Der Auftraggeber bleibt dabei nach § 2 Abs. 8 DSG-LSA rechtlich stets speichernde Stelle und trägt damit auch die Last der Verantwortung (§ 8 Abs. 1 DSG-LSA).

Er hat den Auftragnehmer insbesondere unter Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen und ihn schriftlich zu beauftragen.
Ist auf den Auftragnehmer das DSG-LSA nicht anwendbar (z.B. bei einem privaten Betrieb), so ist der Auftraggeber nach § 8 Abs. 6 DSG-LSA verpflichtet, vertraglich sicherzustellen, daß der Auftragnehmer die Bestimmungen des DSG-LSA befolgt und sich der Kontrolle durch den Landesbeauftragten unterwirft. Außerdem hat der Auftraggeber in einem solchen Fall den Landesbeauftragten über die Beauftragung zu unterrichten. Dies wird häufig vergessen.
Der Landesbeauftragte mußte im Berichtszeitraum bei seinen Kontrollen und Beratungen verschiedene öffentliche Stellen des Landes darauf hinweisen, daß bei der Auftragsvergabe der § 8 DSG-LSA entweder nicht oder nur unzulänglich beachtet wurde. Die Ursache dafür lag weniger in der Unkenntnis datenschutzrechtlicher Regelungen, sondern vielmehr im Unvermögen der Verantwortlichen, in einer Vergabe von Hilfsaufgaben an einen Auftragnehmer eine Verarbeitung personenbezogener Daten im Auftrag zu erkennen und den logischen Schluß der Anwendung des DSG-LSA zu ziehen.

Häufige Fehler bei der Auftragsvergabe waren z.B.

- die fehlende vertragliche Regelung zur Kontrollbefugnis des Landesbeauftragten nach § 8 Abs. 6 DSG-LSA,
- Unterauftragsverhältnisse wurden, wie in § 8 Abs. 2 DSG-LSA gefordert, nicht schriftlich vereinbart,
- keine Prüfung einer erforderlichen Meldung des privaten Auftragnehmers nach § 32 BDSG,
- der vertraglich nicht geregelte Verbleib des Datenbestandes nach Vertragsende,
- die nicht als Datenverarbeitung erkannte Vernichtung von Akten.

Abschließend ist auf die Bereiche hinzuweisen, in denen die Auftragsdatenverarbeitung stark eingeschränkt ist.
So wird in § 80 SGB X die Verarbeitung oder Nutzung von Sozialdaten im Auftrag geregelt und die Auftragsdatenverarbeitung durch nicht-öffentliche Stellen nur in Ausnahmefällen zugelassen.

Eingeschränkt ist auch die Auftragsdatenverarbeitung von Steuerdaten, weil das Steuergeheimnis gem. § 30 AO zu wahren ist. Grundsätzlich soll sie nur bei öffentlichen Stellen möglich sein. In jedem Fall ist eine Verpflichtung der beauftragten Mitarbeiter entsprechend dem Verpflichtungsgesetz erforderlich.

Zur Auftragsdatenverarbeitung hat der Landesbeauftragte ein Informationsblatt erstellt **(Anlage 21).**

13.3 Wartung und Fernwartung von Datenverarbeitungsanlagen

Beim Landesbeauftragten gehen immer wieder Fragen zur rechtlichen Einordnung von Wartung und Fernwartung ein.
Das DSG-LSA enthält dazu bisher keine spezielle Regelung; so ist es auch bei den meisten Datenschutzgesetzen der anderen Bundesländer. Diskutiert wird deshalb seit längerem, ob nicht entweder die bestehenden Vorschriften zur Datenübermittlung oder zur Datenverarbeitung im Auftrag angewendet werden können.

Tendenziell wird die Fernwartung eher der Auftragsdatenverarbeitung zugeordnet.

Der Landesbeauftragte ist der Meinung, daß es sich im Regelfall weder um Datenübermittlung noch um eine Auftragsdatenverarbeitung handelt, weil der Zweck der Fernwartung nicht die Verarbeitung oder Nutzung personenbezogener Daten ist, sondern lediglich die Wartung des EDV-Systems. Es fehlt sowohl dem Auftraggeber einer Wartung als auch dem die Wartung durchführenden Auftragnehmer der Wille zur bewußten Offenbarung der personenbezogenen Daten bzw. der Wille, diese zur Kenntnis zu nehmen.
Nur in Ausnahmefällen kann es dabei zu einer Weitergabe von personenbezogenen Daten bzw. deren Übermittlung kommen. Auch dagegen hilft aber in den meisten Fällen eine vorgehaltene Musterdatei, in der fiktive Daten zur Programmprobe bzw. zu einem Testlauf zur Verfügung stehen.
Sollte dennoch eine Bekanntgabe der Daten im Einzelfall unumgänglich sein, wie z.B. bei der Wiederherstellung oder Neueinprogrammierung einer ganz oder teilweise zerstörten Datei mit personenbezogenen Daten, sind zunächst, zur

Eingrenzung des Problems, Schutzmaßnahmen zu ergreifen (vgl. NJW - CoR - 5/1993, S. 23). Ergänzend können in einem solchen Einzelfall die Regeln zur Auftragsdatenverarbeitung herangezogen werden.

Der Landesbeauftragte wird anhand der aktuellen Diskussion noch prüfen, ob er dazu dem Landtag eine Novellierung des § 8 DSG-LSA empfehlen soll.

13.4 Schutzstufenkonzept für personenbezogene Daten

Die Umsetzung des § 6 Abs. 1 DSG-LSA verpflichtet jede öffentliche Stelle, die selbst oder im Auftrag personenbezogene Daten verarbeitet oder nutzt, die dafür erforderlichen technisch-organisatorischen Maßnahmen zu deren Schutz zu treffen. Dabei sind Maßnahmen nur erforderlich, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck der Daten steht.

Der Schutzzweck wiederum richtet sich neben dem Umfang der zu verarbeitenden Daten insbesondere nach deren **Sensitivität.**

§ 6 Abs. 2 DSG-LSA verlangt von jeder öffentlichen Stelle, die personenbezogene Daten automatisiert verarbeitet, Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind, deren Schutz in angemessener Weise sicherzustellen.

Kriterien für die Einstufung personenbezogener Daten in sog. "Schutzstufen" wurden beim Landesbeauftragten häufig erfragt.
Ein Patentrezept für diese Einstufung gibt es nicht. Generell muß durch jede öffentliche Stelle in Abwägung des Einzelfalles eine eigenverantwortliche Einstufung vorgenommen werden, deren Gründe verständlich und nachvollziehbar sein müssen.
Dabei sind die Grenzen zwischen den einzelnen Sensitivitätsgraden nicht starr, sondern fließend, und es bedarf immer der Gewichtung aller Faktoren bei ihrer Verarbeitung bzw. Nutzung.

Der Landesbeauftragte möchte mit dem Hinweisblatt **(Anlage 20)** Empfehlungen für eine Einstufung personenbezogener Daten geben. Gleichzeitig sind mögliche Schutzmaßnahmen, die keinen Anspruch auf Vollständigkeit erheben, den einzelnen Schutzstufen beispielhaft zugeordnet.

13.5 Einzelthemen des technischen und organisatorischen Datenschutzes

13.5.1 Datenschutz im Besucherverkehr in öffentlichen Behörden und Dienststellen

Eine anlaßbezogene Stichprobe hat verschiedene Verfahrensweisen beim Umgang mit Besucherdaten durch die Pförtnerdienste in den obersten Landesbehörden ergeben. Dies hat der Landesbeauftragte zum Anlaß genommen, diese Behörden in einem Rundschreiben darauf hinzuweisen, daß sich die Zulässigkeit der Erhebung und weiteren Verarbeitung der Besucherdaten nach dem DSG-LSA, im besonderen nach den §§ 9 und 10 DSG-LSA, regelt.

Im Rahmen der danach zu überprüfenden Erforderlichkeit dürfte ohne eine besondere Sicherheitslage bei privaten Besuchern in öffentlichen Stellen die Abfrage von Name, Vorname und Besuchsziel bzw. -zweck und ggf. der Eintrag in eine Liste ausreichen. Ist ein Eintrag erforderlich, soll er durch den Pförtnerdienst erfolgen. Andernfalls erhält der Besucher (ungewollt) Kenntnis von den personenbezogenen Daten anderer Besucher, die sich bereits in der Behörde befinden oder befanden. Allein die Tatsache des Besuches fällt aber bereits unter das Amtsgeheimnis.
Bei Besuchern mit Dienstausweis dürfte eine Notierung von Name, Vorname und Dienststelle nur in Ausnahmefällen erforderlich sein, da es gerade der Sinn des Dienstausweises ist, ohne aufwendige Dokumentation den Zugang zu öffentlichen Stellen zu erleichtern.
Im übrigen wird durch den Landesbeauftragten eine zeitlich unbegrenzte Aufbewahrung der notierten Daten weder für erforderlich noch für verhältnismäßig und damit nach § 16 Abs. 2 Nr. 2 DSG-LSA für unzulässig gehalten. In der Regel wird eine Frist von maximal einem Jahr genügen.
Das Ministerium des Innern hat prompt reagiert und für seinen Geschäftsbereich eine entsprechende Erlaßregelung getroffen.

13.5.2 Datenspeicherung in Telekommunikationsanlagen

Nach den Allgemeinen Richtlinien über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen in Landesbehörden und -dienststellen vom 21.12.1992 (MBl. LSA 1993 S. 1301) sind die Gebührendaten abgehender Wählverbindungen grundsätzlich zu erfassen.
Dabei wird für jede gebührenpflichtige Verbindung nach außen in der Gebührendatei der Telekommunikationsanlage ein sog. Gebührendatensatz gespeichert. Dieser enthält u.a. die Nummer von Anrufer und Angerufenem, Zeitpunkt und Dauer der Verbindung sowie die verursachten Gebühreneinheiten, nicht jedoch Gesprächsinhalte.
Da bei diesem Verfahren auch sensitive personenbezogene Daten verarbeitet werden, hat der Landesbeauftragte eine Telekommunikationsanlage einer Prüfung unterzogen. Schwerpunkt war dabei der Umgang mit den Gesprächsverbindungsdaten, vor allem bei privaten Telefongesprächen der Bediensteten.
Der Landesbeauftragte empfiehlt zur Beachtung datenschutzrechtlicher Bestimmungen dabei folgende Verfahrensweise:

- private Gespräche sind durch Verwendung einer besonderen Kennziffer von Dienstgesprächen zu unterscheiden,
- bei der automatisierten Erfassung der Gebührendaten privater Verbindungen ist die Rufnummer des angerufenen Teilnehmers mindestens um die letzten zwei Ziffern verkürzt zu speichern,
- die Gesprächsgebühren sind in gesonderten Nachweisen für dienstlich sowie für privat angewählte Verbindungen auszuweisen,
- nach Ausdruck der Nachweise sind die gespeicherten Gebührendaten zu löschen, eine Sicherheitskopie wird bis zum Abschluß der Abrechnung aufbewahrt, wobei die nach § 6 Abs. 2 DSG-LSA erforderlichen technischen und organisatorischen Schutzmaßnahmen zu veranlassen sind,
- die Auflistung mit den privaten Gesprächsgebühren ist dem Bediensteten in einem verschlossenen Umschlag oder direkt persönlich auszuhändigen.

Es hat sich im übrigen als zweckmäßig erwiesen, zum Schutz vor Mißbrauch des Nebenstellenanschlusses jedem Mitarbeiter eine Geheimnummer zuzuteilen, mit der er seinen Anschluß sperren kann, soweit die Telekommunikationsanlage über dieses Leistungsmerkmal verfügt.

13.5.3 Richtige Löschung und andere Schutzmaßnahmen

Werden durch die öffentlichen Stellen des Landes personenbezogene Daten automatisiert verarbeitet, sind je nach Art der zu schützenden Daten die in § 6 Abs. 2 Ziffn. 1 bis 10 DSG-LSA genannten technischen und organisatorischen Maßnahmen zu treffen.

Das beinhaltet auch die Pflicht, bei der Löschung nicht mehr erforderlicher Daten ein Verfahren anzuwenden, das - im Rahmen der Schutzwürdigkeit dieser Daten - eine Wiederherstellung unmöglich macht.
Der Landesbeauftragte hat deshalb aus gegebenem Anlaß wiederholt darauf hinweisen müssen, daß physisches Löschen von Daten auf wiederbeschreibbaren Datenträgern nur durch Überschreiben der entsprechenden Datei(en) und der als gelöscht geltenden freien Bereiche des Datenträgers mit einem Hilfsprogramm wirklich sicher erfolgt.
Die Verwendung des DOS-Befehls "DEL" oder von Programmen, die eine analoge Verfahrensweise anwenden, wie z.B. der Dateimanager von MS-WINDOWS, reichen nicht aus.
Besondere Sorgfalt ist geboten, wenn Rechner mit eingebauten Datenträgern (hauptsächlich Festplatten) im Zusammenhang mit Garantie- oder Gewährleistungsansprüchen bzw. im Rahmen von Service- oder Wartungsleistungen an Hersteller, Händler oder Dienstleister übergeben werden müssen. Ist Löschen/ Überschreiben der zu schützenden personenbezogenen Daten auf dem Datenträger nicht möglich, kann es unter Umständen im schutzwürdigen Interesse unbeteiligter Dritter erforderlich sein, den Datenträger aus dem Rechner vorher auszubauen.

13.5.4 Fehler beim Datenträgeraustausch

Dem Landesbeauftragten war bekannt geworden, daß an eine zentrale Stelle des Landes von verschiedenen Absendebehörden täglich ca. 20 Disketten mit personenbezogenen Daten zur Einspeicherung in eine Zentraldatei zugesandt wurden. Das datenschutzrechtliche Problem begann nach der Verarbeitung der Disketteninhalte. Die Disketten wurden ungelöscht und ungeordnet an beliebige Einsender zurückgeschickt.
Erst kurz vor dem Kontrollbesuch des Landesbeauftragten war damit begonnen worden, die Daten mit einer dem DOS-Befehl "DEL" vergleichbaren Löschanweisung des verwendeten Datenbankprogramms zu löschen.
Der Landesbeauftragte mußte die verantwortliche öffentliche Stelle darauf aufmerksam machen, daß auch dies nicht den gesetzlichen Anforderungen entspricht. Derart gelöschte Daten können mit einfachen Tool-Programmen wieder hergestellt werden, und damit liegt eine tatsächliche Löschung im Sinne des DSG-LSA nicht vor.
Erforderlich war, die Disketten nach der Datenübernahme unumkehrbar zu formatieren, die Dateien mit entsprechenden Dienstprogrammen zu überschreiben oder die Disketten mit einer Datei ohne personenbezogene Daten zu füllen, die die vorhandenen Daten überschreibt.

Kurz nach der Kontrolle ist das Verfahren mit der Inbetriebnahme des ITN-LSA eingestellt worden, so daß sich die datenschutzrechtlichen Probleme damit erledigt haben.

13.5.5 Computerviren

Im Rahmen von Kontrollen und Beratungen mußte der Landesbeauftragte im Berichtszeitraum eine steigende Zahl mit Computerviren infizierter PC feststellen. Werden auf diesen PC personenbezogene Daten verarbeitet oder genutzt, liegt ein Verstoß gegen § 14 Abs. 2 Satz 3 DSG-LSA vor. Öffentliche Stellen haben nämlich dafür zu sorgen, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird. Eine Verseuchung mit Computerviren aber stellt eine

ernste Gefahr für die Datensicherheit dar und muß unverzüglich beseitigt werden.

Als größte Schwachstelle im System der durch die öffentlichen Stellen jeweils veranlaßten Maßnahmen zum Schutz der Rechner vor Computerviren erwiesen sich die Benutzer selbst. Neu gelieferte Rechner oder Softwareprodukte wurden ohne vorherige Anwendung von Virensuchprogrammen benutzt, Disketten zwischen Rechnern ausgetauscht, ohne sie vorher auf Infektionen zu untersuchen, Software unbekannter Herkunft, hauptsächlich Spiele, wurde bedenkenlos gestartet und nicht zuletzt war die Wiederherstellung durch Computerviren geschädigter Programme und Datendateien durch nicht oder halbherzig betriebene Backup-Verfahren unmöglich oder unvollständig.

Der Landesbeauftragte hat deshalb empfohlen, vor allem in Bereichen, in denen mit Disketten gearbeitet wird, und dort, wo nicht auszuschließen ist, daß von Disketten Daten oder Programme in einen Rechner geladen werden könnten, Virensuch- und Virenschutzsoftware oder andere PC-Sicherheitsprodukte zu verwenden. Die Verfahren sind ständig und nicht nur sporadisch anzuwenden, und bei einem Virenscanner ist stets die aktuelle Version zu verwenden. Eine Alternative zu Virenscannern stellen Hardwarelösungen (Einsteck-Karten) dar. Ein wesentlicher Vorteil dieser Virenschutzlösung besteht in der einmaligen Installation ohne die Notwendigkeit der ständigen Aktualisierung, die nur bei softwarebasierenden Lösungen (Virenscanner) anzuwenden ist.
Durch das Bundesamt für Sicherheit in der Informationstechnik ist bereits eine Reihe von PC-Sicherheitsprodukten geprüft und zertifiziert worden. Aktuelle Informationen über diese Produkte können bei Bedarf auch beim Landesbeauftragten abgefragt werden.

13.5.6 Aktenvernichtung

Grundlage für die Vernichtung von Datenträgern mit personenbezogenen Daten ist die DIN 32757 vom Oktober 1985. Diese beinhaltet 5 Sicherheitsstufen, in denen die Restpartikelgröße sowie Toleranzbereiche festgelegt sind. Diese DIN

wurde im Oktober 1993 als neuer Entwurf vorgelegt und gab damit Grund zu datenschutzrechtlichen Diskussionen, da die Anforderungen an den Grad der Vernichtung teils abgeschwächt teils verschärft wurden.

Der Landesbeauftragte nahm dies zum Anlaß, sich vor Ort bei einem Aktenvernichtungsunternehmen über die momentane Praxis zu informieren. Hierbei wurde deutlich, daß schon jetzt bei der Sicherheitsstufe 2 das Risiko, auf einem Restpartikel lesbare Daten zu finden, sehr hoch ist, weil es durch die Konstruktion der Messertechnik und die Verwirbelung der zerschnittenen Teile zu unterschiedlich großen - und damit lesbaren - Restteilen kommt.

Die Gefahr, daß gezielt gesuchte personenbezogene Informationen gefunden und deanonymisiert werden, ist dabei relativ gering, aber die Kenntnisnahme und Verwertung von Zufallsfunden ist möglich. Im beobachteten Arbeitsgang wurden nicht nur Akten bzw. Datenträger eines Kunden, sondern mehrerer Kunden innerhalb eines Produktionsballens vernichtet.

Es muß deshalb festgestellt werden, daß zur Vernichtung von sensitiven Daten in Aktenvernichtungsunternehmen nur die Sicherheitsstufe 3 geeignet ist, insbesondere auch im Hinblick auf den neuen Entwurf, der größere Papierpartikel in Sicherheitsstufe 2 und 3 zuläßt. Die öffentlichen Stellen des Landes werden dies bei ihren Aufträgen vertraglich zu regeln haben.

13.5.7 Landesrechenzentrum

Im Rahmen der Einführung landeseinheitlicher Verfahren im Landesrechenzentrum zur Ausführung des Bundesausbildungsförderungsgesetzes (BAföG) und des Wohngeldsondergesetzes im Dezember 1993 bzw. Januar 1994 wurde auch der Landesbeauftragte um Beratung gebeten.

In diesem Zusammenhang wurden Mängel bei der Außensicherung des Gebäudes sowie im Bereich der Transportkontrolle festgestellt. Insbesondere betraf dies die Zugangssicherung zum Versandraum des Rechenzentrums, nicht

verschließbare Transportbehältnisse und die damit bestehende Möglichkeit der unbemerkten und unbefugten Kenntnisnahme von besonders schutzbedürftigen personenbezogenen Daten durch Dritte beim Transport.
Auch die Unversehrtheit und Vollständigkeit des Inhaltes der Transportbehältnisse waren so nach der Anlieferung nicht zu prüfen.

Die Hinweise des Landesbeauftragten wurden beachtet, die Mängel, soweit möglich, sofort behoben. Notwendige bauliche Maßnahmen wurden bei der mittelfristigen Finanzplanung berücksichtigt.

Zur Zeit fehlt noch die dem Landesbeauftragten zugesagte Gesamtsicherheitskonzeption für das Rechenzentrum. Das Ministerium des Innern hat sie jetzt für Ende April 1995 angekündigt.

13.5.8 Grundbucharchiv

Aus gegebenem Anlaß wurde das Grundbucharchiv des Landes Sachsen-Anhalt 1993 vom Landesbeauftragten im Rahmen einer Ortsbesichtigung auf technische und organisatorische Sicherheit geprüft.

Dabei wurden erhebliche Mängel, wie z.B. fehlende Dienstanweisungen zum Umgang mit den Akten, mangelnde Außensicherung des Gebäudes und unzureichende Brandschutzmaßnahmen, festgestellt und das Ministerium der Justiz gebeten, diese unverzüglich im Hinblick auf die gesetzliche Verpflichtung in § 6 Abs. 1 DSG-LSA beseitigen zu lassen.
Bei der Kontrolle ein Jahr später konnte festgestellt werden, daß die entsprechenden baulichen und organisatorischen Maßnahmen umgesetzt wurden und jetzt ein ausreichender Schutz gewährleistet ist.

13.5.9 IT-unterstützte Vorgangsbearbeitung in der Zentralen Bußgeldstelle

Der Landesbeauftragte wurde gem. § 22 Abs. 4 DSG-LSA darüber informiert, daß in der Zentralen Bußgeldstelle beim Regierungspräsidium Magdeburg eine wesentlich veränderte und erweiterte Version der bis dato dort verwendeten Vorgangsbearbeitungssoftware in Betrieb genommen werden sollte.
Die datenschutzrechtliche Prüfung des für die Softwareentwicklung erstellten Pflichtenheftes ergab erhebliche Defizite, z.B. fehlte eine Berücksichtigung der rechtlich vorgegebenen Aufbewahrungs- und Verjährungsfristen. Nach Gesprächen mit dem Regierungspräsidium Magdeburg konnten die Mängel weitgehend ausgeräumt und viele Regelungen klarer gefaßt werden. Zur Zeit fehlt noch die vom Landesbeauftragten geforderte Dienstanweisung für die Anwendung des neuen Verfahrens.

Das Ministerium des Innern hat dem Landesbeauftragten die weitere Information über den Projektverlauf und auch die Erstellung der Dienstanweisung zugesagt. Die Vielzahl der betroffenen Bürger wird auch zukünftig die Aufmerksamkeit des Landesbeauftragten für dieses Verfahren erfordern.

14. Hochschulen

14.1 Diplomprüfungsordnung für Studiengänge Betriebswirtschaftslehre und Volkswirtschaftslehre

Ein Petent wandte sich an den Landesbeauftragten und bat um datenschutzrechtliche Prüfung, was das zuständige Prüfungsamt der Universität als Nachweis der Prüfungsunfähigkeit bei Krankheit verlangen darf. Der ihm zugeleitete Vordruck des Prüfungsamtes verlangte ein ärztliches Attest mit Angaben des Befundes, der Bezeichnung der Krankheit (optional) und den Krankheitssymptomen.
Natürlich darf sich ein Prüfungskandidat nicht wegen angeblicher Erkrankung vor einer unliebsamen Staatsprüfung "drücken", sondern muß seine Erkrankung ggf. nachweisen. Dabei muß er aber nicht mehr angeben, als der Gesetzgeber wohl abgewogen von ihm verlangt.

Rechtsgrundlage für die Vorlage des ärztlichen Attestes ist eine Vorschrift der Diplomprüfungsordnung. Diese verlangt vom Kandidaten lediglich die Glaubhaftmachung der für das Versäumnis oder den Rücktritt von der Prüfung geltend gemachten Gründe - bei Krankheit durch Vorlage eines ärztlichen Attestes.

Die im Verwaltungswege vom Prüfungsamt mit seinem Vordruck vorgenommene Ausdehnung der Angaben auf die Bezeichnung der Krankheit, die Angabe des medizinischen Befundes und der Krankheitssymptome ist durch die eindeutige Formulierung der Prüfungsordnung nicht gedeckt und damit unzulässig. Auch die im Zusammenhang mit der Glaubhaftmachung erforderliche Mitwirkungspflicht des Prüfungskandidaten kann nicht dazu führen, daß auf dem Wege der "Freiwilligkeit" mehr Daten vom Kandidaten gefordert werden, als es der Gesetz- und Verordnungsgeber selbst für erforderlich hält.

Sollten sich im Einzelfall konkrete Hinweise auf ein "unglaubhaftes" Attest ergeben, kann ein amtsärztliches Attest gefordert werden.
Das Prüfungsamt wurde auf die Rechtswidrigkeit des derzeitigen Verfahrens hingewiesen und das Kultusministerium als zuständige Rechtsaufsichtsbehörde informiert.

15. Kommunalverwaltung

15.1 Übermittlung personenbezogener Daten an Private

Ein Petent wandte sich an den Landesbeauftragten, weil er in einem privaten Leserbrief in der lokalen Presse Einzelheiten eines ihn betreffenden Kaufvertrages wiederfand. Im einzelnen wurden Name und Vorname, die vollständige Adresse sowie die Eigentumsverhältnisse zum Flurstück, das verkauft wurde, genannt. Auch die Urkundennummer des Kaufvertrages mit der Treuhandanstalt fand er in diesem Leserbrief ebenso wieder, wie Einzelheiten zum vertraglich geregelten Wegerecht. Diese personenbezogenen Angaben kannte eigentlich nur die örtliche Gemeindeverwaltung und dies aus anderem Anlaß.

Die Nachforschungen des Landesbeauftragten ergaben, daß der Petent die Gemeindeverwaltung nur gebeten hatte, die Mitglieder und Gäste eines örtlichen Vereins darüber zu informieren, daß er ein Überqueren seines Grundstückes ab einem bestimmten Stichtag nicht länger dulden wolle.

Der (ehrenamtliche) Bürgermeister übersah, daß er ohne gesetzliche Grundlage nicht beliebig an einen Privatmann personenbezogene Informationen zur Person des Petenten herausgeben durfte. Die Voraussetzungen für eine Datenübermittlung nach § 12 Abs. 1 DSG-LSA lagen nicht vor.

15.2 Anforderung namentlich ergänzter Stellenbesetzungslisten durch die Kommunalaufsicht

Ein Regierungspräsidium hatte die Kreisverwaltungen seines Bezirkes im Zusammenhang mit der seinerzeit bevorstehenden Kreisgebietsreform um Vorlage von namentlich ergänzten Stellenbesetzungslisten gebeten. Ein datenschutzbewußter Landkreis hat beim Landesbeauftragten die Zulässigkeit hinterfragt.

Ausgangspunkt für die datenschutzrechtliche Prüfung war § 28 Abs. 1 Satz 1 DSG-LSA. Danach muß die Übermittlung personenbezogener Daten zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich sein oder eine Rechtsvorschrift die Übermittlung vorsehen. Nach § 21 Abs. 3 lit. i der bis zum 1. Juli 1994 geltenden Kommunalverfassung vom 17. Mai 1990 - jetzt regeln dies § 73 GO LSA und § 62 LKO LSA - beschließt die zuständige Kommunalvertretung in Wahrnehmung ihrer Personalhoheit über den Stellenplan, der als Anlage dem Haushaltsplan beigefügt wird. Dies gehört zu dem von Art. 28 Abs. 2 GG und Art. 87 Abs. 1 Verf-LSA geschützten Selbstverwaltungsbereich. Umfang und Inhalt des Stellenplanes richten sich nach § 6 GemHVO. Danach ist es haushaltsgesetzlich nicht zwingend, daß der Stellenplan namentliche Angaben zu den Beschäftigten enthält. Auf dieser Grundlage wäre deshalb eine Übersendung namentlicher Stellenbesetzungslisten nicht zulässig gewesen.

Zu berücksichtigen war aber das vom Landtag Sachsen-Anhalt am 13.07.1993 beschlossene Gesetz zur Kreisgebietsreform, wonach mit Wirkung vom 01.07.1994 eine große Anzahl von Landkreisen aufgelöst und neue Landkreisen gebildet wurden.
Dementsprechend hatte das Ministerium des Innern als Kommunalaufsichtsbehörde von der Möglichkeit des § 131 BRRG und § 3 Abs. 1 Satz 2 des Ersten Vorschaltgesetzes zur Verwaltungs- und Gebietsreform des Landes Sachsen-Anhalt vom 9. Oktober 1992 Gebrauch gemacht, stellen- und personalwirtschaftliche Maßnahmen (zeitlich befristet bis maximal 1 Jahr) unter Genehmigungsvorbehalt zu stellen, wenn innerhalb absehbarer Zeit mit einer Umbildung im Sinne des § 128 BRRG zu rechnen war.

Angesichts dieser besonderen Rechtslage und der örtlich und zeitlich befristeten Regelung sowie der vorgesehenen Begrenzung der personenbezogenen Angaben auf Name, Vorname und Funktion hat der Landesbeauftragte keine datenschutzrechtlichen Bedenken gegen eine Übermittlung nach § 28 Abs. 1 Satz 1 DSG-LSA erhoben und die personenbezogene Ergänzung der Stellenpläne als zulässige Zweckänderung nach § 10 Abs. 3 DSG-LSA angesehen.

15.3 Personalauswahlverfahren aus Anlaß der Verwaltungs- und Gebietsreform

Stellenumfang und Stellenstruktur der im Zuge der Verwaltungs- und Gebietsreform des Landes Sachsen-Anhalt neu zu bildenden Landkreise entsprachen vielfach nicht dem vorhandenen Personalbestand. Im Einvernehmen mit den Personalräten wurde deshalb nach Lösungen gesucht, um die Personalauswahl für die Ausstattung der neuen Landkreise auf eine rechtlich sichere Basis zu stellen. In einem Landkreis sollten die Bewerber für die künftige **Leitungsebene** auch Fragen nach ihrer früheren Beschäftigung beantworten. Derartige Fragen wurden bei Bewerbern der nachgeordneten Bereiche nicht gestellt. Der Personalrat des Landkreises, der dem Verfahren grundsätzlich zustimmen wollte, bat deshalb zuvor um datenschutzrechtliche Beurteilung.

Bis zur Umsetzung des Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften vom 11.06.1992 (BGBl. I S. 1030) in Landesrecht gilt in Sachsen-Anhalt für den Umgang mit personenbezogenen Daten bei Bewerbern und Beschäftigten öffentlicher Stellen § 28 Abs. 1 DSG-LSA. Danach ist die Erhebung und Verarbeitung von Personaldaten u.a. zulässig, wenn dies zur Durchführung personeller Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist.
Der im Gesetz genannte Erforderlichkeitsgrundsatz soll dazu führen, daß das Fragerecht des Arbeitgebers sich auf den notwendigen Umfang beschränkt. Der Arbeitgeber kann nach der höchstrichterlichen Rechtsprechung vom Bewerber nur solche Dinge abfragen, an deren Kenntnis er ein berechtigtes, billigenswertes und schutzwürdiges Interesse im Hinblick auf die weitere Gestaltung des Arbeitsverhältnisses hat. Das schließt beispielsweise Umstände aus, die sich auf das Arbeitsverhältnis nicht auswirken, aber auch solche, deren Preisgabe einen übermäßigen Eingriff in die Persönlichkeitssphäre darstellen würde. Dementsprechend dürfen einem Bediensteten nur Fragen vorgelegt und Unterlagen abgefordert werden, auf die es für sein weiteres Beschäftigungsverhältnis ankommt.

Stellen des öffentlichen Dienstes sind - das ist bekannt - nach Eignung, Leistung und Befähigung zu besetzen. Die Dienstvereinbarung zwischen dem Landkreis und dem Personalrat sah deshalb für die Personalauswahl der Amts- und Sachgebietsleiterstellen im neuen Kreis ein besonderes Auswahlverfahren vor, das sich hinsichtlich der Eignung an den Leitrichtlinien, die die Kommunale Gemeinschaftsstelle 1993 erarbeitet hatte, orientieren sollte. Bewertet werden danach der nonverbale und verbale Ausdruck, die Initiative, Aktivität, das systematische Denken und Handeln, die soziale Sensibilität und Kompetenz und Fachkenntnisse im Bereich von Führungswissen und die Fähigkeit zur Umsetzung.

Der Landkreis hielt es zur Feststellung dieser Faktoren nicht für ausreichend, lediglich den bisherigen Werdegang in der Kreisverwaltung "auszuleuchten", vielmehr sei auch wichtig, ob bereits vor dem Eintritt in die Kreisverwaltung Führungsaufgaben ausgeübt wurden. Dies auch deshalb, weil sämtliche Kandidaten als "Seiteneinsteiger" nicht aus der öffentlichen Verwaltung hervorgegangen waren.

Diese Argumentation des Landkreises war sachgerecht und die vorgesehene Verfahrensweise jedenfalls datenschutzrechtlich nicht zu beanstanden.

15.4 Verstoß gegen die Pflicht zur Amtsverschwiegenheit

Ein Bürger, der sein Grundstück verkauft hatte, beschwerte sich darüber, daß der Inhalt des Kaufvertrages zum Gegenstand einer Debatte in einer Sitzung seiner Gemeindevertretung geworden war.

Wie der Landesbeauftragte feststellen mußte, hatte ein Mitglied des Gemeinderates in seiner weiteren Funktion als Landrat von dem Grundstückskaufvertrag Kenntnis erlangt. Einzelheiten daraus hatte er unter Verstoß gegen seine Verschwiegenheitsverpflichtung in der Sitzung des Gemeinderates an die Anwesenden weitergegeben.

Der Landesbeauftragte nimmt diesen Fall zum Anlaß, noch einmal nachdrücklich an die Pflicht zur Verschwiegenheit zu erinnern. Dies ist besonders zu beachten, wenn - wie im geschilderten Fall - im Rahmen einer dienstlichen Tätigkeit zu Recht personenbezogene Informationen zur Kenntnis gelangen, diese aber nicht im Zusammenhang mit einer **anderen** dienstlichen Tätigkeit bekanntgegeben werden dürfen, weil sonst gegen das gesetzliche Gebot der Zweckbindung verstoßen würde.

15.5 Datenübermittlung aus dem Grundbesitzabgabenbescheid an eine Wasser- und Abwasser-GmbH

Mit einer Eingabe rügte ein Petent die Verletzung datenschutzrechtlicher Bestimmungen durch eine Gemeinde, weil diese eine Kopie der Aktenausfertigung des Grundbesitzabgabenbescheides an eine Wasser- und Abwasser-GmbH übermittelt hatte.
Die Übersendung des Abgabenbescheides an die Wasser- und Abwasser-GmbH stellt sich rechtlich als Übermittlung personenbezogener Daten an eine nichtöffentliche Stelle dar und wäre nach § 4 Abs. 1 DSG-LSA nur zulässig gewesen,

wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene vorher eingewilligt hätte.

Zwar ist die Gemeinde nach dem Kommunalabgabengesetz des Landes (KAG-LSA) berechtigt, selbst oder durch Dritte Wasser-/Abwassergebühren festzusetzen und dafür die personenbezogenen Daten der Abgabepflichtigen zu erheben und zu verarbeiten. Voraussetzung ist aber eine entsprechende Satzung als Rechtsgrundlage nach § 2 bzw. § 10 KAG-LSA.
Diese fehlte im vorliegenden Fall. Damit fehlte auch die erforderliche Rechtsgrundlage zur Übermittlung der bei der Gemeinde aus anderen Erhebungszwecken (Grundsteuer) vorhandenen personenbezogenen Daten des Petenten.

Das Verhalten der Gemeinde war zudem aus einem weiteren Grunde rechtswidrig und wegen Verstoßes gegen datenschutzrechtliche Bestimmungen formell zu beanstanden. Es durften auch bei einer rechtlich möglichen Abgabenfestsetzung nur diejenigen personenbezogenen Daten übermittelt werden, die für die Abgabenerhebung erforderlich waren und keinem besonderen Amtsgeheimnis unterlagen. Durch die Übersendung der Kopie des Grundsteuerbescheides des Petenten war auch hiergegen verstoßen worden. Dies stellte einen Verstoß gegen das Steuergeheimnis (§ 30 der Abgabenordnung) dar.

16. Landesregierung und Landtag

Die Wahrnehmung der verschiedenen Aufgaben von Regierung und Parlament im demokratischen Rechtsstaat führt im täglichen Miteinander beider Gewalten zwangsläufig zu ständigen Informationsflüssen. Nicht gerade selten kommt es dabei auch zu einer Übermittlung personenbezogener Daten von Bediensteten, aber auch von betroffenen Bürgerinnen und Bürgern. Sie geraten manchmal auf eigenen Antrag, aber weitaus häufiger ohne ihr Wissen und oft gegen ihren Willen mit ihren ganz persönlichen Anliegen und Daten in ein nicht mehr überschaubares Datenübermittlungskarussell. Dann werden sie häufig nur noch zum

Objekt staatlichen Handelns, und die jeder öffentlichen Stelle obliegende Pflicht, die verfassungsmäßigen Rechte der Betroffenen auf Schutz ihrer Persönlichkeit stets zu beachten, bleibt auf der Strecke. Die folgenden Beiträge geben einen kleinen Überblick zum Problemspektrum.
Es bleibt aber festzustellen, daß gerade in diesem Arbeitsfeld beide Seiten zunehmende Sensibilität und eine große Bereitschaft zur Beachtung des Persönlichkeitsschutzes zeigen, auch über parteipolitische Interessen hinweg.

16.1 Bekanntgabe personenbezogener Daten an Abgeordnete

16.1.1 Schutz bei Kleinen Anfragen

In einer Kleinen Anfrage hatte ein Abgeordneter von der Landesregierung wissen wollen, welcher Dezernent/welche Dezernentin in einer Angelegenheit nach dem Schulgesetz über die dort zugelassenen Ausnahmen entschieden hatte. Die Staatskanzlei, die eine Namensnennung unter Hinweis auf Art. 53 Abs. 4 Landesverfassung verweigerte, bat den Landesbeauftragten um datenschutzrechtliche Beurteilung.

Der Landesbeauftragte hat sich mit folgender Begründung der Ablehnung durch die Staatskanzlei angeschlossen:

Die Beantwortung Kleiner Anfragen durch die Landesregierung erfolgt gem. Art. 53 der Verfassung des Landes Sachsen-Anhalt. Dazu gehört eine erschöpfende sachliche Behandlung der vom Fragesteller unterbreiteten Problematik.
Dabei kann die Landesregierung in die Pflicht geraten, zwischen der weitgefaßten Fürsorgepflicht des Dienstherrn einerseits und der politischen Verantwortung gegenüber dem Parlament andererseits abwägen zu müssen.
Im Regelfall ist es ausreichend, wenn die Landesregierung im Hinblick auf den Grundsatz der Einheit der Verwaltung lediglich die entscheidende Organisationseinheit offenbart. Die Übermittlung personenbezogener Daten eines Bediensteten verbietet sich dann mangels Erforderlichkeit, denn die Verantwortung gegenüber dem Bürger oder dem Parlament obliegt, losgelöst vom einzelnen Bediensteten, der zuständigen Behörde und letztlich der obersten Landesbehörde. Deshalb gilt

auch zugunsten der Landesbediensteten grundsätzlich die Schutzklausel in Art. 53 Abs. 4 Satz 1 Landesverfassung.

Nur im Ausnahmefall kann es erforderlich sein, dem Parlament bzw. nach Art. 53 Abs. 2 der Verfassung dem einzelnen Abgeordneten auch den Namen eines Bediensteten bekannt zu geben. Dafür müßten der Landesregierung aber zur Interessenabwägung seitens des anfragenden Abgeordneten auch besondere Gründe genannt werden (z.B. eine herausragende Funktion des Bediensteten, vorsätzliches rechtswidriges Handeln des Bediensteten mit großer Außenwirkung).

16.1.2 Schutz in den Ausschüssen

Der verfassungsrechtlich gewährleistete Schutz des einzelnen muß auch bei den Erörterungen zwischen der Landesregierung und den Abgeordneten in den Ausschüssen gewährleistet sein. Der Landesbeauftragte mußte deshalb einen Fall aufgreifen, in dem der Vertreter der Landesregierung - teilweise auch auf Nachfragen der Abgeordneten - eine Fülle von Einzelangaben zu den persönlichen und sachlichen Verhältnissen zweier Bediensteter an die Abgeordneten übermittelt hatte. Einige Angaben waren sogar dem dienst- und disziplinarrechtlichen Bereich zuzuordnen, und dies ist der klassische Fall, in dem schutzwürdige Belange besonders eingehend gewichtet werden müssen.
Dafür enthält Art. 53 Abs. 4 der Landesverfassung eine entsprechende Schutzklausel.
In den Fällen, in denen die Landesregierung auch nach intensiver Abwägung die Übermittlung sensitiver Einzelangaben zu einer bestimmten Person für unabweisbar hält, muß in jedem Fall das persönlichkeitsschützende Verfahren nach den §§ 34 und 35 der Geheimschutzordnung des Landtages vom 4. Februar 1993 eingehalten werden. In diesem Verfahren wird nicht nur sichergestellt, daß vor Beginn der Ausführungen der Landesregierung alle Nichtausschußmitglieder den Sitzungssaal verlassen müssen, sondern es wird auch nur eine einzige Niederschrift zu diesem Punkt angefertigt.

Der Landesbeauftragte hat den Fall zum Anlaß genommen, das Problem nicht nur mit dem beteiligten Vertreter der Landesregierung zu erörtern, sondern auch mit Hilfe des parlamentarischen Dienstes nach Wegen zu suchen, die solche Fehler künftig vermeidbar werden lassen.
Entscheidend bleibt dabei die rechtliche Verantwortung der Landesregierung als der übermittelnden Stelle. Von ihr muß der entscheidende Hinweis an die Parlamentarier auf vorgesehene schutzbedürftige Angaben kommen. Unabhängig davon wird aber auch der jeweilige Ausschußvorsitzende seiner Leitungsverantwortung nur dann gerecht werden, wenn er das von Art. 6 Abs. 1 der Landesverfassung gewährte Grundrecht auf informationelle Selbstbestimmung nicht aus dem Auge verliert.

16.2 Übermittlung personenbezogener Daten bei der Bearbeitung von Petitionen

Der Landtag von Sachsen-Anhalt hat im Zusammenhang mit dem Entwurf einer "Gemeinsamen Geschäftsordnung der Ministerien des Landes Sachsen-Anhalt" auch das Petitionsverfahren geregelt und dabei auch den Landesbeauftragten gebeten, Teile des Verfahrens aus datenschutzrechtlicher Sicht zu beurteilen. Insbesondere ging es um die Frage, ob der Name des Petenten in dem notwendigen Schriftverkehr zwischen der Landesregierung und dem Parlament offenbart werden darf. Hierzu wurde folgende Auffassung vertreten:

Mit dem nach Artikel 19 der Verfassung des Landes Sachsen-Anhalt jedermann eingeräumten Recht, sich schriftlich mit Bitten oder Beschwerden an die dort genannten öffentlichen Organe zu wenden, wird dem einzelnen ein formloser Rechtsbehelf garantiert. Zugleich wird dem Parlament eine wirkungsvolle Möglichkeit gegeben, kritisierten Verhaltensweisen staatlicher Stellen nachzugehen. Dabei kann es im Einzelfall erforderlich sein, daß auch der jeweilige Einsender der Petition namentlich gegenüber der betroffenen Stelle genannt werden muß. Der Landtag selbst - beraten durch die Landtagsverwaltung - muß hier seiner Verantwortung gerecht werden und auch unter datenschutzrechtlichen Gesichtspunkten prüfen, ob bei der Weitergabe der Petition an die Landesregierung **in jedem Fall** der Name des Einsenders übermittelt werden muß.

Im Regelfall wird man davon ausgehen dürfen, daß der Einsender auch der Betroffene ist. Ist dies nicht der Fall, muß ggf. geprüft werden, ob nicht die Namen des Einsenders und des Betroffenen vor der Übermittlung an die Landesregierung unkenntlich gemacht werden müssen.
Kommt der Landtag bei seiner Vorprüfung zu dem Ergebnis, daß die Namen des Betroffenen und ggf. des Einsenders für die Bearbeitung der Petition durch die Landesregierung unverzichtbar sind, so müssen die Betroffenen das hinnehmen. Wer selbst eine Petition einreicht, muß bei verständiger Würdigung der erforderlichen Arbeitsabläufe davon ausgehen, daß die Bearbeitung im Regelfall nicht ohne konkreten Bezug zu seiner Person geschehen kann.

Problematischer ist der Fall, in dem ein wohlmeinender Dritter, ohne Wissen eines Betroffenen, zu dessen Gunsten eine "Petition" einreicht und dabei den Namen und andere personenbezogene Daten des Betroffenen angibt. Für diesen Fall ist zu empfehlen, daß die Landtagsverwaltung im vorbereitenden Verfahren nach § 12 Abs. 3 DSG-LSA verfährt und den eigentlich Betroffenen von der vorgesehenen Übermittlung seiner Daten an die Landesregierung in Kenntnis setzt und ihm Gelegenheit gibt, dem Verfahren ggf. zu widersprechen. Sonst liegen möglicherweise die gesetzlichen Voraussetzungen für eine zulässige Datenübermittlung vom Landtag an die Landesregierung nach § 11 Abs. 1 in Verbindung mit § 10 Abs. 2 Nr. 3 DSG-LSA nicht vor.

In jedem Fall muß die Landesregierung - als verantwortliche Stelle die Staatskanzlei - ihrerseits dafür Sorge tragen, daß **nur** die Stellen mit der Bearbeitung der Petition befaßt werden, deren Beteiligung erforderlich ist.

Aber auch in Fällen, in denen bei der Bearbeitung einer Petition Daten Dritter für eine vergleichende Betrachtung herangezogen werden sollen (z.B. bei der Angabe von Vergleichsfällen in Kündigungsverfahren), hat die Landesregierung vor der Übermittlung personenbezogener Daten an den Landtag nach Art. 61 Abs. 2 Satz 2 i.V. mit Art. 53 Abs. 4 Satz 1 der Landesverfassung zu prüfen, ob nicht deren vorherige Einwilligung zur Datenübermittlung einzuholen ist. Handelt es sich bei den Dritten um Landesbedienstete, so können sie sich auf die Regelung in § 56d Abs. 2 BRRG stützen, die Auskünfte nur mit ihrer Einwilligung zuläßt,

es sei denn, daß die Abwehr einer erheblichen Beeinträchtigung für das Gemeinwohl oder der Schutz berechtigter, hochrangiger Interessen des Dritten die Auskunftserteilung zwingend erfordern.

16.3 Anforderungen an ein Petitionsgesetz

Der Petitionsausschuß des Landtages hatte auf Initiative der Landtagsfraktionen in der ersten Legislaturperiode den Auftrag erhalten, den Entwurf eines Petitionsgesetzes für das Land Sachsen-Anhalt zu erarbeiten. Leider kamen die Arbeiten dazu nicht mehr zu einem Abschluß, doch dürften die Bemühungen in dieser Legislaturperiode wieder aufleben.
Insgesamt lassen sich drei Teilbereiche ausmachen, in denen datenschutzrechtliche Regelungen in einem neu zu schaffenden Petitionsgesetz verankert werden sollten:

- Das Recht, sich mit einer Petition direkt an den Landtag zu wenden, sollte auch für Angehörige des öffentlichen Dienstes ohne Einhaltung des Dienstweges gelten. Ferner muß sichergestellt werden, daß Strafgefangene, Sicherungsverwahrte und Untersuchungshäftlinge sich direkt an den Landtag wenden können, ohne daß diese Post durch andere Behörden geöffnet wird.
  Dem Petenten darf durch die Einreichung einer Petition kein Nachteil entstehen.
  Soweit Dritte (z.B. Ehegatte, Pfleger oder Freund) eine Petition einreichen, muß geprüft werden, ob zur Bearbeitung die Einwilligung des Betroffenen eingeholt werden muß. Die Bearbeitung ohne Einwilligung des Betroffenen wäre sonst rechtlich als Verarbeitung personenbezogener Daten ohne Einwilligung zu behandeln. Außerdem könnte sie ihm unter Umständen auch schaden.
- Da bei der Bearbeitung einer Petition im Petitionsausschuß in vielfältiger Weise personenbezogene Daten des Petenten und anderer Personen zur Sprache kommen, empfiehlt der Landesbeauftragte eine gesetzliche Regelung, wonach die Sitzungen des Petitionsausschusses grundsätzlich nicht öffentlich stattfinden und die Bearbeitung der Petition nur durch die Ausschußmitglieder erfolgt.

- Die mit einer Petition offengelegten personenbezogenen Daten dürfen nur zu dem Zweck verarbeitet werden, der in der Bearbeitung der Petition selber liegt. Jede Veröffentlichung der Petition bzw. einer Entscheidung zur Petition darf ohne vorherige Zustimmung durch den Petenten nicht personenbezogen erfolgen.
  Soweit der Petitionsausschuß die Petition an Dritte (außerhalb des Parlaments oder an andere Ausschüsse und Gremien) weiterleiten will, muß er die vorherige Zustimmung des Petenten zu dieser Verfahrensweise einholen.

17. Landwirtschaft

17.1 Das Kontrollsystem InVeKoS

In seinem I. Tätigkeitsbericht hatte der Landesbeauftragte unter dem Thema "Der gläserne Landwirt" (S. 81 f) das Integrierte Verwaltungs- und Kontrollsystem (InVeKoS) zur Landwirtschaftsförderung wegen seiner offensichtlichen Risiken für die Privatsphäre des einzelnen problematisiert.

Hinsichtlich der Gestaltung der Antragsformulare hatte er gegenüber dem Ministerium für Ernährung, Landwirtschaft und Forsten auf allgemein verständliche Formulierungen unter Berücksichtigung der besonderen gesetzlichen Vorschriften des DSG-LSA Wert gelegt.
Zwischenzeitlich hat das Ministerium die Antragsformulare "Agrarförderung 1994" und "Agrarförderung 1995" vorgelegt. Der "Antrag Agrarförderung 1995" enthält nun eine eindeutig formulierte "Erklärung zur Datenverarbeitung", leider fehlen aber noch Hinweise auf die gesetzlichen Bestimmungen des DSG-LSA.

Auch in einem weiteren Punkt haben sich die Bedenken des Landesbeauftragten bestätigt. Der jetzt vorliegende Bericht zum Test der Satellitenerkundung für das Gebiet des Landes Sachsen-Anhalt weist aus, daß 93 % der gestellten Anträge der Landwirte 1992 als zweifelhaft oder falsch gewertet wurden - tatsächlich hat die Überprüfung der "falschen Fälle" vor Ort aber nur 10 % Mängel ergeben!

Inzwischen hat das Ministerium den Landesbeauftragten von der Absicht unterrichtet, im Rahmen der verwaltungsinternen Prüfung der vorgelegten Anträge die Bewirtschaftungsberechtigung des Antragstellers für eine Fläche und deren Katasterangaben in einem automatisierten Verfahren mit den Daten des automatisierten Liegenschaftsbuches abgleichen zu lassen.
Da dieses möglicherweise mit datenschutzrechtlichen Problemen behaftet ist, wird der Landesbeauftragte mit dem Ministerium demnächst ein Gespräch dazu führen.

17.2 Landwirtschaftliche Betriebe - Ermittlung von Primärdaten

Das Ministerium für Ernährung, Landwirtschaft und Forsten bat den Landesbeauftragten um Prüfung eines "Formblattes zur Ermittlung von Betriebsübersichten im Obst- und Gemüsebau des Landes".

In dem vom Ministerium gewählten Verfahren werden nur zum Teil personenbezogene Daten, die außerdem wenig sensitiv sind, erhoben. Weil gleichzeitig auf die Freiwilligkeit der Abgabe des Formblattes hingewiesen und die vorherige Zustimmung der Betroffenen eingeholt wird, hat der Landesbeauftragte keinen Grund gesehen, die vorgelegten Formblätter zu beanstanden.

18. Personalwesen

18.1 Veröffentlichung von Personalnachrichten im Ministerialblatt

Ziff. 6.6 Abschnitt IV der Richtlinien der Landesregierung über das Verkündungs- und Veröffentlichungswesen (MBl. LSA 1992, S. 105) sah vor, daß Personalnachrichten ab der Besoldungsgruppe A 15 bzw. vergleichbarer Vergütungsgruppen im Ministerialblatt veröffentlicht werden konnten. Mit der Absicht, künftig von einer Veröffentlichung gänzlich abzusehen, hatte die Staatskanzlei auch den Landesbeauftragten um Stellungnahme gebeten.

Dieser hat die vorgesehene Zurückhaltung der Landesregierung bei der Veröffentlichung von Personaldaten begrüßt. Das Problem bestand letztlich in einer Abwägung der dienstlichen Interessen des Landes mit den persönlichen Schutzinteressen der Bediensteten.

Grundsätzlich ist die öffentliche Verwaltung in einem freiheitlich demokratischen Staat transparent. Daraus folgt auch, daß Bedienstete es im dienstlichen Interesse hinnehmen müssen, daß wenig sensitive personenbezogene Grunddaten - wie Name und Funktion in der Behörde - im Zusammenhang mit dienstlichen Entscheidungen Dritten übermittelt und damit bekannt werden.
Gleiches gilt auch für Bedienstete, die herausgehobene Funktionen bekleiden oder in dem ihnen zugewiesenen Aufgabenbereich wichtige Entscheidungsträger sind.

In allen anderen Funktionsbereichen und im persönlichen Bereich aller Bediensteter greift heute das Recht auf informationelle Selbstbestimmung mit seiner Ausprägung in den bereichsspezifischen Einzelgesetzen zugunsten des Persönlichkeitsschutzes ein. Dabei hat der Gesetzgeber bewußt das Persönlichkeitsrecht der öffentlichen Bediensteten gestärkt.
So dürfen nach § 56 Abs. 1 BRRG Personalaktendaten nur für Zwecke der Personalverwaltung oder Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in die anderweitige Verwendung ein.
Wenn auch die genannte Vorschrift noch vom Landesgesetzgeber als eigenständige Regelung umzusetzen ist, sollten die darin enthaltenen Grundsätze bereits jetzt in Sachsen-Anhalt berücksichtigt werden.
Auch der jetzt noch übergangsweise geltende § 28 Abs. 1 DSG-LSA, der die Datenerhebung, -verarbeitung und -nutzung öffentlicher Stellen bei Dienst- und Arbeitsverhältnissen regelt, grenzt die Möglichkeiten der Übermittlung personenbezogener Daten der Bediensteten an außenstehende Dritte bereits erheblich ein.
Bereits 1992 wurde deshalb dem Ministerium der Justiz im Zusammenhang mit einer geplanten Veröffentlichung personenbezogener Daten im bundesweit erscheinenden Handbuch der Justiz dringend empfohlen, ohne Zustimmung des Bediensteten nur den Namen im Zusammenhang mit der Behörde abzudrucken.
Der Vorgang ist im I. Tätigkeitsbericht (S. 91) angesprochen worden.

Inzwischen werden Personalnachrichten im Ministerialblatt nicht mehr veröffentlicht.

18.2 Personalvermittlung durch Übermittlung unzulässiger Daten per Telefax

Eine oberste Landesbehörde hatte per Telefax bei den Personalreferaten anderer oberster Landesbehörden um Mitteilung gebeten, ob dort für einen bestimmten Bediensteten eine freie Stelle des höheren bzw. gehobenen Dienstes verfügbar war. Dazu war eine als "Kurzbiographie" bezeichnete Beschreibung der betroffenen Person mit einer Fülle personenbezogener Daten einschl. der Parteizugehörigkeit beigefügt. Auch wenn der Name des Betroffenen, der im übrigen nicht eingewilligt hatte, nicht genannt wurde, ließen sich durch die detaillierte Darstellung ohne größeren Aufwand Rückschlüsse auf die Person ziehen. Damit galt das Gesetz zum Schutz personenbezogener Daten der Bürger (§ 2 Abs. 1 DSG-LSA).

Den gesetzlichen Vorgaben entsprach das Verfahren im vorliegenden Fall weder in rechtlicher (§ 28 Abs. 1 Satz 1 DSG-LSA) noch in technischer Hinsicht (§ 6 DSG-LSA).
Es ist im Personalwesen des öffentlichen Dienstes ständige Praxis, personelle Dispositionen im Einzelfall nur in den wesentlichen Grundpositionen (Status, bisherige dienstliche Verwendung und ggf. berufliche Vorbildung) offen zu kennzeichnen und im übrigen (vgl. § 28 Abs. 1 Satz 3 DSG-LSA) nur in Absprache mit dem Betroffenen personenbezogene Daten zu übermitteln bzw. auf die Einsichtnahme in die Personalakte zu verweisen.

Da eine Personalauslese nach § 8 BG-LSA und der entsprechenden BAT-Regelung ausschließlich nach Eignung, Befähigung und fachlicher Leistung vorzunehmen ist, sind im übrigen Hinweise auf eine politische Anschauung oder die Mitgliedschaft in einer politischen Vereinigung unzulässig.

Was die technische Datensicherheit anbetrifft, so ist die Übermittlung personenbezogener Daten per **Telefax** generell als ein nach § 6 DSG-LSA unzuverlässiges Verfahren einzustufen. Der Landesbeauftragte hat deshalb wiederholt

Landesbehörden darauf hinweisen müssen, daß die Übermittlung solcher Daten per Telefax nur in absoluten Ausnahmefällen in Frage kommen kann. Ein solcher Ausnahmefall war hier nicht ersichtlich.

18.3 Datenübermittlung aus Personalunterlagen an Gerichte

Im Zusammenhang mit Kündigungen von Arbeitsverhältnissen in einer Kommune sind in großer Zahl auch sensitive Personaldaten unbeteiligter Dritter an die Öffentlichkeit gelangt. Der Vorgang hat breites Interesse in der örtlichen und überörtlichen Presse erfahren und war Gegenstand einer Prüfung durch den Landesbeauftragten. Letztlich konnte nicht definitiv festgestellt werden, ob die Daten von der Kommune oder über das Arbeitsgericht unberechtigt an die Öffentlichkeit gelangt sind.

Dieser Fall hat den Landesbeauftragten veranlaßt, die mit der Bearbeitung von Personalangelegenheiten befaßten öffentlichen Stellen auf den sorgfältigen Umgang mit den ihnen von ihren Beschäftigten anvertrauten Personaldaten hinzuweisen. Er hat deshalb auf die mit dem Bekanntwerden von Daten unbeteiligter Dritter bei Kündigungsschutzprozessen und sog. Konkurrentenklagen auftretende grundsätzliche Problematik in einer Bekanntmachung hingewiesen. Die Bekanntmachung ist als **Anlage 22** abgedruckt.

18.4 Videoaufzeichnungen von Lehramtsanwärtern

Ein Petent, der sich als Lehramtsanwärter in einem Ausbildungsseminar befand, fragte den Landesbeauftragten, ob eine von ihm gehaltene Unterrichtsstunde ohne vorherige Absprache mit ihm auf Video aufgezeichnet werden dürfe, um anschließend zu Ausbildungszwecken am Ausbildungsseminar eingesetzt zu werden.

Der Landesbeauftragte hat dazu folgende Auffassung vertreten:

Nach § 84a Abs. 2 Schulgesetz i.V. mit § 28 Abs. 1 DSG-LSA dürfen Daten von Beschäftigten nur erhoben, verarbeitet oder genutzt werden, wenn dies u.a. zur

Durchführung des Dienstverhältnisses erforderlich ist. Der Einsatz von Videoaufzeichnungen im Ausbildungsseminar erfolgt im Rahmen der Ausbildung von Lehramtsanwärtern als Mittler zwischen erziehungswissenschaftlicher Theorie und schulischer Praxis. Da nach § 2 der Verordnung über die Zweite Staatsprüfung für Lehrämter in der Staatsprüfung festgestellt werden soll, ob der Prüfling nach seinen Kenntnissen und Fähigkeiten als Lehrer für das von ihm durch sein Studium und seine schulpraktische Ausbildung angestrebte Lehramt befähigt ist, können auch Videoaufzeichnungen als didaktisch geeignetes Mittel zur Ausbildung angesehen werden. Da insoweit die gesetzlich geforderten Voraussetzungen vorliegen, bestehen aus datenschutzrechtlicher Sicht gegen die Erhebung und Verarbeitung der Aufnahmen des Betroffenen auf einem Bildträger und dessen Aufbewahrung für die Dauer des persönlichen Ausbildungsabschnittes keine Bedenken.

Schwieriger ist es, wenn die Videoaufzeichnungen auch für die Schulung anderer Auszubildender im Ausbildungsseminar verwendet werden sollen. Zwar läßt § 10 Abs. 3 Satz 2 DSG-LSA eine solche Zweckänderung bei der Verwendung der Daten zu, doch können überwiegende schutzwürdige Interessen des Betroffenen gegen eine solche Verwendung sprechen.

Es ist deshalb richtig, wenn die ausbildende Behörde und das Kultusministerium erklärt haben, es solle generell das Einverständnis des Lehramtsanwärters vor der Aufzeichnung eingeholt werden.

18.5 Aushändigung von Originalmitteilungen der sog. Gauckbehörde an die Betroffenen

Nach § 21 Abs. 1 Nr. 6d StUG erhalten Behörden Auskünfte vom Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (sog. Gauckbehörde) über die bei ihnen beschäftigten Mitarbeiter. An einen Landkreis war nun die Bitte eines Bediensteten herangetragen worden, die Bescheinigung der Gauckbehörde, daß keine Erkenntnisse vorliegen, an ihn auszuhändigen. Der Landesbeauftragte hat die Frage unter zwei Gesichtspunkten geprüft:

a) Die Mitteilung wird im Regelfall Teil der Personalakte und gehört zur vorangegangenen Anfrage der Behörde. Die Aushändigung der Originalmitteilung berührt damit die Rechtsfrage, inwieweit die Entnahme von Vorgängen aus Personalakten zulässig ist.

Die zuständigen obersten Bundesgerichte haben in der Vergangenheit mehrfach entschieden, daß sich das Recht und die Pflicht einer Behörde zur **vollständigen** Aktenführung aus ihrer jeweiligen Aufgabenzuweisung ergibt (vgl. z.B. NJW 1983, 2135). Die Gerichte haben dabei darauf abgestellt, daß die Vorgänge rechtmäßig in die Akten gelangt sind und ein sachlicher Bezug zur Aufgabenerfüllung der personalaktenführenden Stelle besteht.
Dieses gilt grundsätzlich auch für die Überprüfung der Mitarbeiter einer Behörde auf Tätigkeit beim ehemaligen Ministerium für Staatssicherheit, jedenfalls solange die speziellen Unterlagen der Überprüfung wesentlicher Teil der Personalakte sind. Daraus folgt, daß grundsätzlich eine nachträgliche Entfernung oder Abgabe von vorhandenen Unterlagen oder Teilen von ihnen nicht zulässig ist.
Im übrigen würde die Entfernung auch dem Gebot wahrheitsgetreuer Nachzeichnung des bisherigen Geschehens und der zukünftigen Verhaltensweise widersprechen. Überdies ist eine korrekte Aktenführung für die Durchführung der allgemeinen Aufsicht und der speziellen Rechtskontrolle, wie sie z.B. auch vom Landesbeauftragten für den Datenschutz vorgenommen werden kann, unerläßlich.

Diese von der Rechtsprechung für die Beamten aufgestellten Grundsätze gelten nach § 13 BAT-O im gleichen Umfang für Angestellte im öffentlichen Dienst.

b) Es bestehen aber keine Bedenken, dem betroffenen Bediensteten eine Ablichtung, die den Voraussetzungen des § 12 Abs. 5 StUG entspricht, auszuhändigen. Hiernach darf nur eine Ablichtung ausgehändigt werden, in der keine personenbezogenen Informationen über andere Betroffene oder Dritte vorhanden sind.

18.6 Fragebogen zur Personalauswahl bei Kündigungen

Die leider in vielen Bereichen des öffentlichen Dienstes notwendig gewordene Reduzierung der Stellen führt in nicht seltenen Fällen auch zu datenschutzrechtlichen Problemen, wenn der Arbeitgeber im Bemühen um sozialverträgliche Auswahlkriterien zusätzliche personenbezogene Daten bei seinen Arbeitnehmern erhebt und dabei nicht beachtet, daß dann auch die gesetzlich vorgesehenen Regelungen zum Schutz des Persönlichkeitsrechts beachtet werden müssen.
So verteilte eine Gemeinde an alle Mitarbeiterinnen ihrer kommunalen Kinderbetreuungseinrichtungen einen Fragebogen, in dem personenbezogene Angaben über das Dienst- bzw. Arbeitsverhältnis (Beschäftigungszeit, Qualifikation, Familienstand), Angaben aus dem Privatbereich (Alleinverdiener, Pflege von Familienangehörigen, besondere Lasten aus Unterhaltsverpflichtungen u.ä.) und im dritten Teil eine Eigenbeurteilung gefordert wurden.

Die anlaßbezogene Kontrolle und die anschließende Besprechung mit der Gemeinde ergaben zusätzliche Anhaltspunkte, um der Gemeinde ein datenschutzgerechtes Verfahren empfehlen zu können:

Neben dem Hinweis auf den Anlaß für eine solche Befragung muß den Bediensteten stets gesagt werden, ob die Beantwortung der Fragen freigestellt ist oder sich auf eine gesetzliche Grundlage stützt. Diese muß dann benannt werden, damit sie der Betroffene ggf. selbst nachlesen oder rechtlich überprüfen lassen kann.
Nur ausnahmsweise ist es zulässig, bereits beim Arbeitgeber vorhandene Personaldaten erneut zu erheben, weil sonst gegen das Verbot der Doppeldatenerhebung bzw. der Vorratsdatenhaltung verstoßen wird.
Soweit Angaben aus dem privaten Lebensbereich gefordert werden, die in keinem Bezug zum Arbeitsverhältnis stehen, müssen die Voraussetzungen für eine ordnungsgemäße Einwilligung nach § 4 Abs. 2 DSG-LSA beachtet werden. Auch bei freiwilliger Angabe dürfen nur Einzelangaben aus dem Privatbereich erfragt werden, die nach der Rechtsprechung der Arbeitsgerichte ein zulässiges Kriterium für die Auswahl darstellen. So ist z.B. die Frage: "Haben Sie zu Hause einen großen oder kleinen Garten?" nicht zulässig.

Im konkreten Fall war es auch nötig darauf hinzuweisen, daß Personaldaten und personenbezogene Unterlagen nur in **einer** Personalakte im Personalamt zu führen sind (vgl. § 90 BG-LSA bzw. § 13 BAT) und nicht daneben noch in einer weiteren Datensammlung im Fachamt, in dem der Bedienstete beschäftigt ist.

Im konkreten Fall wurde in Zusammenarbeit mit dem Landesbeauftragten ein neuer Vordruck entwickelt, und die bis dahin unzulässig erhobenen und gespeicherten Daten wurden nach § 16 Abs. 2 DSG-LSA gelöscht.

18.7 Frauenfördergesetz

Das Gesetz zur beruflichen Förderung von Frauen im öffentlichen Dienst des Landes Sachsen-Anhalt (Frauenfördergesetz) vom 07.12.1993 (GVBl. LSA S. 734) trat am 14.12.1993 in Kraft. Der Landesbeauftragte wurde rechtzeitig beteiligt und seine Anregungen wurden berücksichtigt.

Wegen des notwendigen besonderen Schutzes von Personaldaten hat der Gesetzgeber ein Akteneinsichtsrecht für die Gleichstellungsbeauftragten nur mit Zustimmung des Betroffenen vorgesehen. Das gleiche gilt für die Bewerbungsunterlagen, so daß beiden Personenkreisen der gleiche Schutz ihrer personenbezogenen Merkmale zugestanden wird.

Auch für die durch Verwaltungsvorschrift geregelte Ausführung des § 20 Frauenfördergesetz gab der Landesbeauftragte einen Hinweis. Bei der Bestandsaufnahme für die Erstellung des Frauenförderplanes sind keine personenbezogenen Daten erforderlich.

19. Personalvertretung

19.1 Mitbestimmung bei der Einführung von Informationstechnik (IT)

Daß die gleichzeitig mit der Bildung neuer Behörden eingeführte IT auch datenschutzrechtliche Probleme aufwerfen kann, verdeutlicht die Anfrage eines

Personalrates zur Mitbestimmung bei der Installation einer Telefondatenerfassungsanlage.

Die Installation einer solchen Anlage ist mitbestimmungspflichtig, wenn die Voraussetzungen des § 69 Nr. 2 PersVG LSA vorliegen, also die Einrichtung u.a. dazu bestimmt ist, das Verhalten oder die Leistung der Beschäftigten zu überwachen. Die Möglichkeit einer solchen Kontrolle genügt (Beschluß des Bundesverwaltungsgerichts vom 16. Dezember 1987 - BVerwG 6P 32.84).
Werden der Apparat des Mitarbeiters, die angerufene Zielnummer, Beginn und Ende des Gespräches sowie die anfallenden Gebühren für dienstliche und privat geführte Gespräche gespeichert, so könnte durch die Telefondatenerfassung kontrolliert werden, in welchem Umfang die Arbeit für private Zwecke unterbrochen wird. Die Einrichtung eines Gebührencomputers zur Aufzeichnung von Telefongesprächen stellt daher eine technische Einrichtung dar, die sowohl geeignet als auch dazu bestimmt ist, das Verhalten der Beschäftigten zu überwachen (Grabendorff/Windscheid/Ilbertz/Widmaier: Bundespersonalvertretungsgesetz, 7. Auflage 1991, S. 740). Der Personalvertretung steht daher ein Mitbestimmungsrecht schon bei der Einführung des neuen Erfassungssystems zu.
Unabhängig von der vorstehend abgehandelten Grundsatzfrage hat die Personalvertretung auch ein Mitbestimmungsrecht in den beim Gebrauch der Telefondatenerfassung auftretenden Einzelproblemen. Rechnungen über Privatgespräche dürfen offen nur direkt zwischen dem für die Abrechnung der Gespräche zuständigen Bearbeiter und dem einzelnen Betroffenen übergeben werden; in allen anderen Fällen (z.B. bei Boteneinsatz) ist die Abrechnung nur im verschlossenen Umschlag zu übermitteln.

Zur Lösung dieser und anderer Probleme bei der Gebührendatenerfassung und Auswertung von Telefongesprächen bietet es sich an, die für den Bereich der unmittelbaren Landesverwaltung geltenden "Allg. Richtlinien über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen in Landesbehörden und -dienststellen" (vgl. Ziff. 13.5.2) in einer Betriebsvereinbarung zwischen dem Personalrat und der Behörde/ Dienststelle für entsprechend anwendbar zu erklären. Die Allg. Richtlinien sind inhaltlich mit dem Landesbeauftragten abgestimmt.

20. Polizei

20.1 Entwurf eines Gesetzes über das Bundeskriminalamt (BKA)

Dem BKA obliegt es u.a., die Zusammenarbeit zwischen Bund und Ländern bei der Bekämpfung der über die Ländergrenzen hinweggehenden Kriminalität sicherzustellen. Der von der Bundesregierung Anfang 1995 vorgelegte Gesetzentwurf für ein neues BKA-Gesetz zielt darauf ab, die seit langem überfälligen bereichsspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung, insbesondere im Informationssystem INPOL, in das Gesetzgebungsverfahren einzubringen.
Dies wird von den Datenschutzbeauftragten des Bundes und der Länder begrüßt.

Bedauerlicherweise ergibt aber die nähere Prüfung des Entwurfs, daß damit auch die seit langem bekannten Bemühungen des Bundes fortgesetzt werden, sich zu Lasten der im Polizeirecht zuständigen Länder und ohne Änderung des Grundgesetzes mehr Kompetenzen im Bereich der Gefahrenabwehr zu schaffen und die Rechte der Länderpolizeien zu beschneiden. Dies hätte auch erhebliche Auswirkungen auf den datenschutzrechtlichen Schutz der Bürger, wenn es im Zuge der Gesetzesberatungen nicht noch zu wesentlichen Änderungen kommt.

Der Landesbeauftragte hat gegenüber dem Ministerium des Innern zu dem Gesetzentwurf Stellung genommen, der sich derzeit zur ersten Beratung im Bundesrat befindet.

Die wesentlichen datenschutzrechtlichen Forderungen ergeben sich aus der Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 9./10.03.1995 **(Anlage 14).**

20.2 Einsatz von Vertrauenspersonen (V-Personen)

Auch in Sachsen-Anhalt bedient sich die Polizei sog. V-Personen. Der Landesbeauftragte wurde von einem Landtagsabgeordneten dazu um Information gebeten und hat sich zusammenfassend wie folgt geäußert:

Als V-Person wird in dem dazu ergangenen Gemeinsamen Runderlaß des Ministeriums des Innern und des Ministeriums der Justiz vom 08.07.1994 (MBl. LSA S. 2017) eine Person bezeichnet, die, ohne einer Strafverfolgungsbehörde anzugehören, bereit ist, diese bei der Aufklärung von Straftaten auf längere Zeit vertraulich zu unterstützen, und deren Identität grundsätzlich geheimgehalten wird. V-Personen werden in der Regel von einem Polizeibeamten geführt und erheben für diesen quasi im Auftrag Einzelinformationen aller Art von Personen, bei denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß sie Straftaten von erheblicher Bedeutung begehen werden oder über Personen, die möglicherweise mit einer solchen Person in Verbindung stehen oder treten werden oder die sich im räumlichen Umfeld einer Person aufhalten, die im besonderen Maße als gefährdet erscheint.

Rechtlich stellt sich die Tätigkeit der V-Person als besondere Form der Datenerhebung dar, die in § 18 Abs. 1, 5 und 6 SOG LSA geregelt ist. Was die Datenerhebung durch V-Personen rechtlich so problematisch macht, ist zum einen, daß der Staat damit vom Regelprinzip abweicht, wonach er im Bereich der Gefahrenabwehr und der Strafverfolgung dem Störer oder Straftäter grundsätzlich mit eigenen Bediensteten und offen gegenüber tritt, zum anderen die Tatsache, daß V-Leute als Privatpersonen sich beim Sammeln personenbezogener Daten nicht an gesetzliche Regeln halten müssen und unerkannt bleiben. Durch den sie führenden Beamten sind sie nur schwer kontrollierbar und im Normalfall wenig zuverlässig, weil sie bei der Arbeit oft eigene Ziele verfolgen (Doppelinformanten) und dies im Prinzip nur um ihres eigenen Vorteils (Strafverschonung, -erleichterung, Geldzuwendungen) wegen tun.

Die Erkenntnisse, die sie liefern, sind wegen ihrer nur begrenzten Verwendbarkeit im Strafprozeß im Regelfall nur Einstiegsgrundlagen für weitere zielgerichtete eigene Ermittlungen von Polizei und Staatsanwaltschaft.

Die genannten gesetzlichen Vorschriften und die dazu erlassenen Verwaltungsvorschriften sind andere Vorschriften über den Datenschutz nach § 22 Abs. 1 Satz 1 DSG-LSA; die Arbeit mit V-Personen unterliegt damit grundsätzlich auch der Kontrolle durch den Landesbeauftragten.

20.3 Transport erkennungsdienstlicher Unterlagen

Der Landesbeauftragte erhielt Hinweise aus einem anderen Bundesland, daß dort der Versand von erkennungsdienstlichen Unterlagen (ed-Unterlagen) von den örtlichen Polizeidienststellen an das LKA sowie zwischen diesem und dem BKA mittels einfachen Briefes vorgenommen wird.

Die Feststellungen beim LKA Sachsen-Anhalt bestätigten auch hier Schwachstellen beim Versand zwischen dem LKA und dem BKA. Hingegen war der Transport von den Polizeidienststellen des Landes zum LKA ausreichend sicher.
Der Landesbeauftragte hat dem LKA Sachsen-Anhalt empfohlen, den Versand der ed-Unterlagen zwischen dem BKA und dem LKA sicherer zu gestalten. Das LKA Sachsen-Anhalt hat inzwischen seine Praxis datenschutzgerecht geändert.

20.4 Wahllichtbildvorlagen im strafrechtlichen Ermittlungsverfahren

Wie der Landesbeauftragte bereits in seinem I. Tätigkeitsbericht (S. 110) ausgeführt hat, gibt es ernsthafte Zweifel an der Zulässigkeit der Wahllichtbildvorlage in der bisherigen Form, weil dafür die erforderliche Rechtsgrundlage in der Strafprozeßordnung bis heute fehlt und auch kein Einverständnis der Betroffenen vorliegt.

Zwischenzeitlich hat der Landesbeauftragte bei der Prüfung einer Polizeibehörde festgestellt, daß dort die Durchführung von Wahllichtbildvorlagen durch eine besondere Dienstanweisung geregelt ist. Auch diese kann den Rechtsmangel nicht ersetzen.

Der Landesbeauftragte hat deshalb gegenüber dem Ministerium der Justiz und dem Ministerium des Innern zum Ausdruck gebracht, daß er die bisherige Verfahrensweise als unzulässig ansieht.

Das Ministerium des Innern hat zwischenzeitlich dazu erklärt, es sehe mangels geeigneter Alternativverfahren derzeit keine Möglichkeit, auf die bisherige Praxis der Wahllichtbildvorlage zu verzichten. Ergänzend wird auf die jüngste obergerichtliche Rechtsprechung der Oberlandesgerichte Karlsruhe und Frankfurt verwiesen, die davon ausgehen, daß die dem Gesetzgeber eingeräumte Übergangsfrist zur Schaffung einer gesetzlichen Grundlage für die Datenverarbeitung im Strafverfahren noch nicht abgelaufen ist.

Für die Übergangszeit strebt das Ministerium des Innern eine landeseinheitliche Regelung an.
Eine Stellungnahme des Ministeriums der Justiz steht zur Zeit noch aus.

20.5 Aufzeichnung aller Telefonanrufe bei der Polizei

Das Brandenburgische Ministerium des Innern hat ein Verfahren in Kraft gesetzt, nach dem im dortigen LKA und den Polizeipräsidien alle eingehenden Telefonanrufe automatisch aufgezeichnet werden.
Dies widerspricht der bisherigen Verfahrensweise in den meisten Bundesländern, wonach vorrangig in Lagezentren bestimmte Telefonleitungen an Aufzeichnungsgeräte für Zwecke der Gefahrenabwehr oder der Strafverfolgung gekoppelt sind.
Der Landesbeauftragte hält die Verfahrensweise in Brandenburg für rechtlich nicht gedeckt und hatte das Ministerium des Innern (MI) um Auskunft gebeten, ob in Sachsen-Anhalt eine solche Totalerfassung praktiziert wird oder deren Einführung beabsichtigt ist.

Nach der dem Landesbeauftragten vorliegenden Stellungnahme ist nicht beabsichtigt, eine Erfassung **aller** eingehenden Telefonanrufe bei der Polizei vorzunehmen. Aufgezeichnet werden aber alle Anrufe, die über den Notruf 110 zur Polizei gelangen. In einem Erlaß hat das MI die Polizeibehörden und -dienststellen darauf hingewiesen, daß - außer im Einzelfall bei Meldungen

über Not- oder Gefahrensituationen - eine Aufzeichnung des Telefonats unzulässig ist, es sei denn, der Anrufer hat der Aufzeichnung zugestimmt.
Nach dem Ergebnis einer zwischenzeitlichen Umfrage des Ministeriums bei den Polizeibehörden und -dienststellen des Landes wird diese Anweisung aber noch nicht überall umgesetzt. Das MI wird daher einen Erlaß erarbeiten, der die zu beachtenden Besonderheiten bei der Aufzeichnung von Telefonanrufen regelt. Der Landesbeauftragte wird zu dem Erlaßentwurf Stellung nehmen.

20.6 Datenübermittlung der Polizei an die Führerscheinbehörde

Im I. Tätigkeitsbericht (S. 105) ist von dem gemeinsamen Runderlaß der Ministerien des Innern, für Wirtschaft, Technologie und Verkehr und für Arbeit und Soziales vom 28.08.1992 und der Berichtspflicht der Polizei an die Führerscheinbehörden in den Fällen berichtet worden, in denen sie im Zusammenhang mit der Führung von Kraftfahrzeugen Drogen oder den Konsum von Drogen feststellt.

Dieses Verfahren erscheint erforderlich und ist im Regelfall auch datenschutzrechtlich unbedenklich. Nur in einem Punkt hatte der Landesbeauftragte das Ministerium des Innern um Klarstellung gebeten:
Das Vorhandensein von Drogen im Pkw läßt nicht in jedem Fall den Rückschluß auf die Drogenabhängigkeit des Pkw-Besitzers zu. Gerade bei mehreren Pkw-Insassen kann nicht davon ausgegangen werden, daß der Pkw-Fahrer auch immer Kenntnis oder die tatsächliche Verfügungsgewalt über mitgeführte Drogen hat.

Mit dem neuen Runderlaß des Ministeriums des Innern, des Ministeriums für Wirtschaft und Technologie und des Ministeriums für Arbeit, Soziales und Gesundheit vom 01.07.1994 (MBl. LSA S. 1954) wurde dieser Kritikpunkt nun ausgeräumt.

20.7 Kriminalakten

Der Landesbeauftragte hat Anfang 1993 begonnen, bei der Polizei die Führung und Haltung der Kriminalakten, die Umsetzung der Bereinigung des DORA-Bestandes sowie die Nutzung der Informationstechnik zu überprüfen (vgl. I. Tätigkeitsbericht S. 112).

Die Überprüfungen wurden im Berichtszeitraum bei den zwei Polizeidirektionen und den sechs Polizeiinspektionen fortgesetzt. Dabei wurde auch die Umsetzung der Bereinigung des „DORA-Bestandes“ überprüft.
Das Daten-Informationssystem „DORA“ wurde in der Kriminalpolizei der ehemaligen DDR ab Mai 1989 eingeführt. Umfang und Inhalt der Daten waren von den damaligen Rechtsgrundlagen und -auffassungen geprägt und entsprachen nicht den rechtsstaatlichen Anforderungen. Aufgrund der durchzuführenden Rechtsangleichungen war es letztendlich nicht sinnvoll, die dem Land Sachsen-Anhalt aus der ehemaligen Zentraldatei des GLKA in Berlin zur Verfügung gestellten Datenbestände des „DORA-Systems“ fortzuführen.
Deshalb hatte das LKA Sachsen-Anhalt als Fachaufsichtsbehörde den kriminalaktenführenden Polizeidienststellen eine zügige Bereinigung des Kriminalaktenbestandes aufgegeben und anschließend die Löschung des Datenbestandes im System „DORA“ durch Überschreiben der Festplatte verfügt. Mit Ausnahme einer Polizeiinspektion war dies zum Zeitpunkt der jeweiligen Kontrolle des Landesbeauftragten auch umgesetzt.

Für die Bereinigung der alten Kriminalakten sowie für die Auskunft aus diesen erließ das LKA am 27.09.1991 entsprechende Richtlinien. Diese waren nach Feststellung des Landesbeauftragten für die Praxis sehr hilfreich und im Vergleich mit den anderen neuen Bundesländern einmalig.

Demgegenüber verzögerte sich die Herausgabe der zu überarbeitenden KpS-Richtlinien durch das Ministerium des Innern trotz ständiger Anmahnungen des Landesbeauftragten bis in das Frühjahr 1994 (vgl. Ziff. 20.10). Bis dahin standen den kriminalaktenführenden Dienststellen nur allgemeine Arbeitshinweise des LKA zur Verfügung sowie im Einzelfall alte KpS-Richtlinienentwürfe aus Niedersachsen.

Bei der stichprobenhaften Prüfung der bereinigten Kriminalakten fiel denn auch auf, daß übernommene Teile aus den Altakten - insbesondere Vernehmungsprotokolle - nicht ausreichend überarbeitet worden waren. Diese Fälle mußten aufgrund der Beanstandung durch den Landesbeauftragten erneut überarbeitet werden.
Beanstandungen ergaben sich auch, weil die Löschung der PKZ nicht vorgenommen und die Abschlußberichte der Strafvollzugsanstalten häufig nicht entfernt waren. Ferner wurde festgestellt, daß die Meldung zum bundesweiten Kriminalaktennachweis häufig nicht berechtigt war.
Auch fehlte vielfach in den Akten der aktuelle POLIS-Auszug.

Bei einer Dienststelle mußte beanstandet werden, daß dort generell eine Aussonderungsprüffrist von 10 Jahren für alle Kriminalakten festgelegt worden war. Dies entsprach nicht § 32 Abs. 4 SOG LSA, wonach eine abgestufte Festsetzung der Fristen je nach Schwere der Tat und persönlichen Eigenschaften des Täters zu erfolgen hat.
Fehlberechnungen gab es auch bei der Festlegung der Aussonderungsprüffrist, weil oft das wichtige Datum der Haftentlassung nicht gesehen oder nicht mehr vermerkt war.

Inzwischen gibt es die mit dem Landesbeauftragten abgestimmte Verordnung über Prüffristen bei polizeilicher Datenspeicherung (Prüffristenverordnung) vom 20.12.1993, die eine datenschutzgerechte Handhabung der Aussonderungsprüffristen in der polizeilichen Praxis gewährleistet.

Ferner fehlte in den übernommenen Akten häufig der Lichtbildnachweis und die Verfügung über die erkennungsdienstliche Behandlung. Beide Punkte waren bei der Kriminalaktenhaltung nach altem DDR-Recht ohne Bedeutung und konnten deshalb systembedingt bei den bereinigten Altakten nicht vorliegen. Die neue Rechtslage erfordert aber eine einheitliche und umfassende Bereinigung, wenn die Kriminalakte nach Ablauf der Frist zu vernichten ist.
Dazu gehört auch die vollständige Vernichtung aller Lichtbilder des Betroffenen. Dies ist nur möglich, wenn alle zur Person vorhandenen Negative, die Zahl der gefertigten Abzüge und ihr Verbleib eindeutig dokumentiert sind.

Bei den künftigen Überprüfungen durch den Landesbeauftragten wird sich zeigen, inwieweit diese Anregungen und Hinweise Beachtung gefunden haben. Positive Ansätze waren bei einigen Polizeidienststellen bei einer späteren Überprüfung bereits erkennbar.

Bezüglich der Anmerkungen zum technischen und organisatorischen Kontrollteil wird auf Ziff. 13.1 verwiesen.

20.8 Zusammenarbeit zwischen Polizei und Verfassungsschutz

Die Polizei und der Verfassungsschutz haben - insbesondere bei der Bearbeitung und beim Umgang mit den sog. Staatsschutzdelikten - Berührungspunkte, die Regelungen für die gemeinsame Zusammenarbeit zwischen beiden erforderlich machen.
Die Rechtsgrundlagen für diese Zusammenarbeit enthält das Verfassungsschutzgesetz des Landes Sachsen-Anhalt vom 14.07.1992 in den §§ 16 und 17.

Einzelheiten der informationellen Zusammenarbeit betreffend die Melde- und Informationswege sind in den Runderlassen des Ministeriums des Innern vom 03.06.1994 (MBl. LSA S. 1517) und vom 13.02.1995 (MBl. LSA S. 390) festgelegt.
Der Landesbeauftragte hat zu beiden Regelungen Stellung genommen, seine Anregungen sind übernommen worden.

20.9 Ausführungsbestimmungen zum SOG LSA

Der Landesbeauftragte ist bei der Erarbeitung der Ausführungsbestimmungen zum SOG LSA vom Ministerium des Innern beteiligt worden. Dabei wurden insbesondere die aus datenschutzrechtlicher Sicht relevanten Ausführungsbestimmungen zu den §§ 14 bis 34 SOG LSA einer genaueren Prüfung unterzogen. Insgesamt kann gesagt werden, daß die inzwischen veröffentlichten Ausführungsbestimmungen vom 24.11.1993 (MBl. LSA 1994, S. 13) aus datenschutzrechtlicher Sicht zu keinen größeren Beanstandungen mehr Anlaß gaben. Die

vom Landesbeauftragten gegebenen Anregungen und Hinweise wurden entsprechend berücksichtigt.

20.10 KpS-Richtlinien

Der Landesbeauftragte kann hierzu zunächst auf seine Ausführungen im I. Tätigkeitsbericht (S. 108) verweisen. Ergänzend ist mitzuteilen, daß seit dem 10.02.1994 endlich die vom Landesbeauftragten seit langem geforderten grundlegenden Verwaltungsvorschriften als Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen vom Ministerium des Innern in Kraft gesetzt worden sind (MBl. LSA S. 1343). Sie stellen eine wesentliche Ergänzung der im zweiten Teil des SOG LSA enthaltenen gesetzlichen Grundlagen dar. Allein in Kriminalakten sind personenbezogene Informationen über rund 149.400 Personen enthalten.

Der Landesbeauftragte hat deshalb in den dazu zuvor geführten zahlreichen Besprechungen zum Teil bis ins Detail gehende datenschutzrechtliche Gesichtspunkte aufzeigen können. Diese sind in vielen Fällen in konkrete Regelungen für die polizeiliche Praxis umgesetzt worden, so daß jetzt von datenschutzgerechten Arbeitsgrundlagen in diesem wichtigen Bereich ausgegangen werden kann.

20.11 Duplikatakten

Der Landesbeauftragte hatte in seinem I. Tätigkeitsbericht (S. 109) zu den datenschutzrechtlichen Grundfragen bei der Verwendung von Duplikatakten durch Dienststellen der Polizei Stellung genommen und gegenüber dem Ministerium des Innern (MI) angeregt, nähere Einzelheiten unter Beteiligung des Ministeriums der Justiz (MJ) zu erörtern.

Das MJ räumt in seiner jetzt dazu vorliegenden Stellungnahme ein, daß die Strafprozeßordnung dazu bisher keine spezielle Regelung trifft. Es möchte aber die Zulässigkeit der Anlegung von Duplikatakten in bestimmten Fällen nicht

ausschließen, wenn dies das Verfahren fördert, weil die Akten bzw. Duplikatakten verschiedenen Stellen, die sie gleichzeitig benötigen, zur Verfügung gestellt werden können. Dies sei etwa der Fall, wenn neben laufenden polizeilichen Ermittlungshandlungen staatsanwaltliche oder richterliche Entscheidungen zu treffen sind oder wenn mehreren Stellen (Verteidigern, Sachverständigen, Versicherungen) Akteneinsicht zu gewähren ist. In solchen Fällen soll § 10 Abs. 1 DSG-LSA als Rechtsgrundlage dienen.
Rechtliche Probleme sieht auch das MJ, wenn das Anlegen und Vorhalten von Duplikatakten nur als Gedächtnisstütze für die ermittelnden Beamten mit der Möglichkeit für eine etwaige spätere Zeugenvernehmung dienen soll.
Der Landesbeauftragte hält deshalb an seiner Auffassung fest, daß die Anlegung von Duplikatakten auf Ausnahmefälle beschränkt bleiben muß. Dabei kann § 10 Abs. 1 DSG-LSA allenfalls **übergangsweise** als Rechtsgrundlage in Betracht kommen, bis die erforderlichen datenschutzrechtlichen Regelungen in der StPO geschaffen worden sind. Bis dahin sollten die vom MJ anerkannten Ausnahmefälle in einer landesweiten gemeinsamen Regelung von MJ und MI festgeschrieben werden, damit die polizeiliche Praxis einen klaren Orientierungsrahmen hat.

20.12 Vernichtung von Kriminalakten und Löschung von Altdaten in INPOL und POLIS

Aus den Beständen der ehemaligen DDR sind eine Vielzahl von Akten und Dateien übernommen worden, die von der ehemaligen Volkspolizei insbesondere zu Zwecken der Strafverfolgung und des Erkennungsdienstes geführt worden waren.
Diese Datensammlungen wurden auf der Grundlage des heute geltenden Rechts nach dem 03.10.1990 bereinigt. Diejenigen Daten, die auch nach rechtsstaatlichen Grundsätzen gespeichert werden durften, sind in die Kriminalakten übernommen und in INPOL bzw. POLIS gespeichert worden. Ihre weitere Behandlung richtet sich nach den Bestimmungen des SOG LSA, insbesondere nach den Regelungen in § 32 Abs. 2 und 4 SOG LSA i.V. mit der Prüffristenverordnung.

Das Ministerium des Innern (MI) aber sah zu Recht datenschutzrechtliche Probleme hinsichtlich der weiteren Behandlung derjenigen Altakten/Altdatensätze, die nicht mehr erforderlich sind. Sie dürfen dann nicht gelöscht bzw. vernichtet, sondern nur gesperrt werden, wenn Grund zu der Annahme besteht, daß schutzwürdige Interessen des Betroffenen beeinträchtigt werden, z.B. wenn seitens des Betroffenen die vorhandenen Daten zu Rehabilitierungszwecken genutzt werden sollen (§ 32 Abs. 7 SOG LSA).
In einer gemeinsamen Besprechung mit dem MI wurden deshalb die verschiedenen Rechtsprobleme erörtert und folgende Vorgehensweise festgelegt:
Die in INPOL und POLIS gespeicherten Altdatensätze werden gelöscht. Die bereinigten Altakten, die wegen des Ablaufs der Prüffristen auf ihre weitere Erforderlichkeit geprüft wurden und deren Aufbewahrung für polizeiliche Zwecke nicht mehr erforderlich ist, werden nicht vernichtet, sondern im Hinblick auf die zeitlich beschränkte Geltung des Strafrechtlichen Rehabilitierungsgesetzes (StrRehaG) bis zu dessen Auslaufen (derzeit Dezember 1995) gesperrt aufbewahrt, um die eventuelle Geltendmachung von Rehabilitierungsansprüchen zu ermöglichen.

Zwischen dem Ministerium des Innern und dem Landesbeauftragten wird noch ein abschließender Katalog erstellt, der festlegt, aus welchem Anlaß Einsicht in die gesperrten Akten gewährt bzw. Auskunft daraus erteilt werden kann.

20.13 Durchführung von Schülerpraktika bei der Polizei

An den Landesbeauftragten ist mehrfach die Frage herangetragen worden, inwieweit Schüler- und Jurastudenten am praktischen Polizeidienst teilnehmen können. Wegen der datenschutzrechtlichen Fragen bei der Durchführung des Praktikums für **Jurastudenten** vgl. Ziff. 21.18.

Schülerpraktika sind nicht nur für deren Berufsentscheidung von Bedeutung, sondern auch aus polizeilicher Sicht wichtig für die Nachwuchsgewinnung.
Aus datenschutzrechtlicher Sicht ist es wünschenswert, Schüler während ihrer Praktikantenzeit bei einer Polizeidienststelle bzw. bei der Teilnahme am Streifendienst der Polizei nur über die Tatsachen zu unterrichten, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Dieses Ziel in die Praxis umzusetzen, dürfte aber nicht ohne wesentliche Einschränkungen bei der Durchführung des Praktikums möglich sein. Ob es dann noch realitätsnah ist und Interesse beim Schüler wecken kann, ist fraglich.

Die entsprechenden Probleme wurden mit dem Ministerium des Innern eingehend erörtert. Insbesondere stellt sich bei minderjährigen Schülern die Frage nach der rechtlich wirksamen Verpflichtung auf den Datenschutz. Die Schüler müßten zunächst vor der Aufnahme des Praktikums mit den Grundzügen des Datenschutzrechts vertraut gemacht werden. Sie sind dabei darüber zu unterrichten, daß der Umgang mit personenbezogenen Daten Vertraulichkeit und Verschwiegenheit gebietet. In keinem Fall sollten sie Einblick in Ermittlungsvorgänge im Zusammenhang mit Sexual-, Gewalt- und Kapitaldelikten erhalten.

Das Ministerium des Innern wird dazu in Kürze einen Erlaß herausgeben.

21. Rechtspflege

Fast 12 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 werden im Bereich der Justiz - vor allem im Bereich der Strafrechtspflege - nach wie vor personenbezogene Daten ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.
Es gibt nur zwei erwähnenswerte Ausnahmen:
Im Zivilrecht wurden durch das Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis vom 15.07.1994 die gesetzlichen Grundlagen für die Speicherung im und Auskünfte aus dem Schuldnerverzeichnis geschaffen (vgl. Ziff. 21.2).
Auf dem Gebiet des Strafrechts wurden mit dem Verbrechensbekämpfungsgesetz vom 28.10.1994 die gesetzlichen Grundlagen für ein staatsanwaltschaftliches Verfahrensregister in der Strafprozeßordnung geschaffen. Im Rahmen der Beratungen zu diesem Gesetz gelang es, die vorgesehene erhebliche Einschränkung des Grundrechts auf informationelle Selbstbestimmung und des Schutzes der Wohnung durch die erweiterten Möglichkeiten zum Abhören von Gesprächen in oder aus Wohnungen abzuwehren. Nicht zuletzt hatten die

Datenschutzbeauftragten des Bundes und der Länder auf ihrer Konferenz vom 26./27.10.1993 - mit Gegenstimme Bayerns - ausdrücklich an ihrer ablehnenden Entschließung zum Großen Lauschangriff festgehalten.

Im Verbrechensbekämpfungsgesetz wurden aber auch die Befugnisse des für die Auslandsaufklärung zuständigen Bundesnachrichtendienstes (BND) in einer datenschutzrechtlich bedenklichen Weise erweitert.
Wer in Deutschland mit dem Ausland telefoniert, muß jetzt damit rechnen, daß der BND die nicht leitungsgebundenen Fernmeldegespräche mithört und hierüber Aufzeichnungen anfertigt, soweit es um strafbare Handlungen im Zusammenhang mit Terrorismus, Verbreitung von Kriegswaffen, Betäubungsmittelimport, internationale Geldwäsche oder Geldfälschung geht.
Das erscheint zunächst nicht so problematisch, hat aber rechtliche und tatsächliche Haken. Das uns alle schützende Post- und Fernmeldegeheimnis (Art. 10 GG) wird ohne Beteiligung eines Richters durchbrochen und, wegen des vom Gesetzgeber nur grob gesteckten Rahmens, muß damit gerechnet werden, daß eine große Zahl Unbeteiligter namentlich erfaßt und u.a. an die Polizei gemeldet wird. Damit werden die aus rechtsstaatlichen Gründen bisher getrennten Aufgabenbereiche beider Behörden vermischt.
Die Datenschutzbeauftragten des Bundes und der Länder haben daher in einer besonderen Entschließung gefordert, das Trennungsgebot in der Gesetzgebung und auch bei der Durchführung der Fernmeldeaufklärung des BND strikt zu beachten **(Anlage 12).** Leider ist der Bundesgesetzgeber dem nicht gefolgt.

Erhebliche datenschutzrechtliche Lücken bestehen im Bereich der Strafrechtspflege weiterhin bei

- der Datenverarbeitung in Strafverfahren, insbesondere in automatisierten Dateien,
- den Datenübermittlungen von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen
- der Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien und der
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb mit Beschluß vom 26./27.09.1994 den Gesetzgeber wegen der mit der Datenerhebung, -verarbeitung und -nutzung verbundenen Rechtseingriffe aufgefordert, zum Schutz des einzelnen unverzüglich dazu bereichsspezifische Regelungen sowie die organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, die der Gefahr einer Verletzung des Persönlichkeitsrechts des Bürgers entgegenwirken **(Anlage 10).**

In Ergänzung der Ausführungen im I. Tätigkeitsbericht (S. 120) kann mitgeteilt werden, daß die Datenschutzbeauftragten mit Beschluß vom 9./10. März 1995 auch eine gesetzliche Regelung über Aufbewahrungsbestimmungen für Justizakten und über die Speicherung personenbezogener Daten in Dateien angemahnt haben **(Anlage 15).**

21.1 Justizmitteilungsgesetz

Die Gerichte und Staatsanwaltschaften des Landes übermitteln in Verfahren der streitigen Zivilgerichtsbarkeit, in der freiwilligen Gerichtsbarkeit und in Strafsachen in einer Vielzahl von Fällen personenbezogene Daten aus und über eingeleitete Verfahren und Maßnahmen an die unterschiedlichsten Stellen. Der Landesbeauftragte kann dazu zunächst auf seine Ausführungen im I. Tätigkeitsbericht (S. 117) verweisen. Die dafür dringend erforderliche (bundes-) gesetzliche Regelung fehlt immer noch.
Der erste und eher lustlose Entwurf der Bundesregierung für ein Gesetz über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (JuMiG) wurde in der letzten Legislaturperiode nicht mehr abschließend behandelt. Nach neuesten Erkenntnissen soll jetzt im Frühsommer diesen Jahres vom Bundeskabinett ein neuer Entwurf beraten und dann dem Bundesrat zur ersten Stellungnahme zugeleitet werden.

Beim Landesbeauftragten häufen sich indessen die Eingaben von überraschten Bürgern, die sich darüber beschwerten, daß sie betreffende Datenübermittlungen auf der Grundlage der MiStra vorgenommen wurden und dies zum Teil für sie zu arbeitsrechtlichen Konsequenzen führte.

Nicht weniger wichtig ist die gesetzliche Grundlage für Mitteilungen von Klagen, Vollstreckungsmaßnahmen u.a. gegen Angehörige rechtsberatender Berufe an die Justizverwaltung und die Standesvertretungen, weil für derartige Übermittlungen zum Schutz der Bürger und des Rechtsverkehrs ein dringendes Bedürfnis besteht.

21.2 Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis

In seinem I. Tätigkeitsbericht (S. 127) hatte der Landesbeauftragte auf die datenschutzrechtlichen Probleme bei der Erteilung von Abschriften aus dem Schuldnerverzeichnis hingewiesen.

Inzwischen hat der Bundesgesetzgeber mit dem am 1. Januar 1995 in Kraft getretenen Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis vom 15. Juli 1994 eine ausreichende Rechtsgrundlage für die Führung, Eintragung, Löschung, Auskunftsersuchen und die Erteilung von Abdrucken und Listen aus dem Schuldnerverzeichnis geschaffen. Man findet die neuen Bestimmungen in den §§ 915 bis 915h ZPO.

Das Gesetz enthält einen vertretbaren Kompromiß zwischen den einander entgegengesetzten Interessen des Betroffenen, seine wirtschaftlich schwierige Lage möglichst wenig bekanntwerden zu lassen, und den Belangen des Wirtschaftsverkehrs, hierüber unterrichtet zu sein.
Besonders wesentlich ist nach Auffassung des Landesbeauftragten die klare Festlegung der möglichen Empfänger von Abdrucken und Listen und deren Unterwerfung unter eine anlaßfreie Kontrolle der für die Überprüfung der Einhaltung der datenschutzrechtlichen Vorschriften zuständigen Stellen.

Mit der Verordnung über das Schuldnerverzeichnis vom 15. Dezember 1994, die ebenfalls am 01.01.1995 in Kraft getreten ist, hat das Bundesministerium der Justiz von seiner Ermächtigung aus dem neuen § 915h Abs. 1 ZPO Gebrauch gemacht und detaillierte Regelungen über den Inhalt des Schuldnerverzeichnisses, den Bezug von Abdrucken und Listen, die Aufbewahrungsmodalitäten, Löschungspflichten und Kontrollmöglichkeiten sowie das Verfahren zur Erteilung

der Bewilligung zum Bezug der Abdrucke und Listen und die Erteilung von Einzelauskünften im automatisierten Abrufverfahren getroffen.
Der Schutz der Daten in und aus dem Schuldnerverzeichnis dürfte mit dieser Verordnung so ausgestaltet worden sein, daß Mißbräuche weitgehend ausgeschlossen sind.

Der Landesbeauftragte wird im Rahmen seiner Kontrollbefugnisse die Umsetzung der neuen Vorschriften über das Schuldnerverzeichnis in der Praxis kritisch begleiten.

21.3 Ehescheidungsverbundurteile und Datenschutz

Aufgrund der gesetzlichen Regelungen in den §§ 623, 629 ZPO ergeht in Scheidungssachen in der Regel ein Ehescheidungsverbundurteil.
Dies bedeutet, daß sowohl über die Scheidung als auch über daraus resultierende Folgesachen zwischen den Ehegatten **eine** gerichtliche Entscheidung ergeht. Solche Verbundurteile sind von den Parteien bei verschiedenen Behörden und sonstigen Stellen (Meldebehörde, Standesamt, Finanzamt, Arbeitgeber etc.) vorzulegen. Wenn dort das vollständige Urteil vorgelegt wird, erhält die betreffende Stelle - neben den von ihr benötigten Angaben - zwangsläufig zusätzlich eine Vielzahl von Informationen - zum Teil höchst sensitiver Art.

Der Landesbeauftragte hat aus diesem Grunde gegenüber dem Ministerium der Justiz (MJ) angeregt, Ehescheidungsverbundurteilen gem. §§ 623, 629 ZPO künftig ein Merkblatt beizufügen, das die Parteien, die zur Regelung weiterer Rechtsangelegenheiten die Ausfertigung eines Urteils benötigen, auf die Möglichkeit der Erstellung von Ausfertigungen ohne Tatbestand und Entscheidungsgründe gem. § 317 Abs. 2 Satz 2 ZPO hinweist. Auf diesem Wege kann sichergestellt werden, daß die Parteien eigenverantwortlich bestimmen, wer welche Daten aus dem Ehescheidungsverbundurteil zur Kenntnisnahme erhält.

Das MJ hat diese Anregung aufgegriffen und mitgeteilt, es habe sie an das Oberlandesgericht Naumburg mit der Bitte um Umsetzung weitergeleitet. Darüber hinaus sei es in Sachsen-Anhalt auch gängige Praxis, nur auf besonderen Antrag hin Urteile mit Tatbestand und Entscheidungsgründen zu erstellen.

21.4 Einsichtnahme in das Grundbuch

Nach § 12 GBO ist jedem die Einsicht in das Grundbuch gestattet, der ein berechtigtes Interesse darlegt. Diese Regelung ist eine spezielle gesetzliche Grundlage zur Datenübermittlung an Dritte. Bereits in seinem I. Tätigkeitsbericht (S. 126) hatte der Landesbeauftragte auf die Probleme hingewiesen, die mit der Einsicht in die personenbezogenen Unterlagen des Grundbuches verbunden sind. Er hat daher in Übereinstimmung mit den Datenschutzbeauftragten des Bundes und der Länder die Auffassung vertreten, daß die Einsichtnahme in das Grundbuch protokolliert werden sollte, damit ggf. eine nachträgliche Kontrolle über deren Rechtmäßigkeit möglich ist.

Der Bundesgesetzgeber ist dieser Empfehlung bisher nicht nachgekommen. Im Rahmen der vom Bundesministerium der Justiz erlassenen Verordnung zur Änderung der Grundbuchverfügung ist nur eine Protokollierung von Abrufen aus dem automatisiert geführten Grundbuch aufgenommen worden, nicht jedoch bei der Einsichtnahme in die noch von Hand geführten Urkundsbücher.

Der Landesbeauftragte hat daher gegenüber dem Ministerium der Justiz (MJ) angeregt, entsprechend einer Regelung in Schleswig-Holstein, auch in Sachsen-Anhalt im Wege eines Erlasses eine Protokollierungspflicht für Einsichtnahmen in die Grundbücher gem. § 12 GBO vorzusehen.

Das MJ hat diese Anregung unter Hinweis auf die bundesrechtlich abschließende Regelung zur Einsichtnahme in die Grundbücher in den Vorschriften der Grundbuchordnung, die auch die Wirksamkeit eines Erlasses in Frage stellen würde, nicht aufgegriffen. Es hat vielmehr darauf hingewiesen, daß das Bundesministerium der Justiz den Entwurf einer Verordnung zur Änderung des Grundbucheinsichtsrecht angekündigt habe, mit dem auch das Anliegen des Datenschutzes aufgegriffen werden solle.

Der Landesbeauftragte stimmt mit dem MJ darin überein, daß einer bundeseinheitlichen Rechtsgrundlage der Vorzug zu geben sein wird. Dabei wird es darauf ankommen, wie eine Regelung gefunden werden kann, die geeignet ist, datenschutzrechtliche Grundanforderungen zu erfüllen, ohne die Arbeit der Grundbuchämter erheblich zu behindern. Das gilt insbesondere auch in einem neuen Land wie Sachsen-Anhalt, in dem die Grundbuchämter sich noch im personellen Aufbau befinden.

21.5 Zustellung von Pfändungs- und Überweisungsbeschlüssen durch Gerichtsvollzieher

§ 35 Ziff. 1 der Geschäftsanweisung für Gerichtsvollzieher (GVGA) regelt die Zustellung von Pfändungs- und Überweisungsbeschlüssen durch Gerichtsvollzieher an Behörden, juristische Personen, Gesellschaften und sonstige Personenmehrheiten. Dabei wird der Gerichtsvollzieher in den überwiegenden Fällen weder den Leiter noch den gesetzlichen Vertreter der entsprechenden Behörde antreffen. In diesen Fällen darf der Gerichtsvollzieher gem. § 35 Ziff. 1 Satz 2 GVGA die Zustellung auch an dort anwesende Beamte oder Bedienstete vornehmen.

Der Landesbeauftragte hat gegenüber dem Ministerium der Justiz (MJ) darauf hingewiesen, daß diese Praxis nur dann nicht unter datenschutzrechtlichen Gesichtspunkten zu beanstanden ist, wenn die Zustellung an die für die Abgabe der Drittschuldnererklärung zuständige Person erfolgt (z.B. Lohnbüro). Wird dagegen die Zustellung an zufällig anwesende Personen vorgenommen (z.B. Pförtner), so muß § 36 Ziff. 3 GVGA Anwendung finden, wonach die Übergabe bzw. Niederlegung nur nach vorherigem Verschließen des Schriftstückes erfolgen darf. Der Landesbeauftragte hat daher angeregt, diesen datenschutzrechtlichen Hinweis bei der Anwendung der §§ 35 und 36 GVGA im Rahmen der Aus- und Fortbildung der Gerichtsvollzieher zu berücksichtigen und ggf. durch eine Änderung bzw. Klarstellung der Geschäftsanweisung für Gerichtsvollzieher umzusetzen.

Das MJ hat diesen Hinweis aufgegriffen. Eine Änderung der Regelungen der GVGA hielt es jedoch nicht für erforderlich. Es hat vielmehr veranlaßt, daß im Rahmen der Aus- und Fortbildungsmaßnahmen für Gerichtsvollzieher auf die Problematik hingewiesen wird.

21.6 Pfändung von EDV-Anlagen durch Gerichtsvollzieher

Datenschutzrechtliche Probleme kann es bei der Pfändung und Verwertung von EDV-Anlagen bzw. deren Zubehör geben, wenn dabei Datenträger mit personenbezogenen Daten des Vollstreckungsschuldners oder gar unbeteiligter Dritter vorhanden sind. Diese können sich auf den in die Rechner eingebauten Festplatten bzw. Wechselfestplatten sowie auf Magnetbändern oder Disketten befinden. Auch wenn nach Auskunft des Ministeriums der Justiz (MJ) die Pfändung von EDV-Anlagen in Sachsen-Anhalt bisher die Ausnahme war, hat der Landesbeauftragte darum gebeten, folgende Schutzmaßnahmen zu beachten:
Zunächst soll dem Vollstreckungsschuldner Gelegenheit gegeben werden, den gespeicherten Datenbestand zu kopieren, um ihn später weiter nutzen zu können. Anschließend ist es geboten, die noch gespeicherten personenbezogenen Daten mit einem Verfahren tatsächlich physisch so zu löschen, daß ein Wiederherstellen der Daten unmöglich ist (vgl. Ziff. 13.5.3).
Fehlt hierzu die erforderliche Fachkunde bei der vollstreckenden Stelle, muß auf die Unterstützung zentraler DV-Stellen des Landes zurückgegriffen werden.

Die für die Vollstreckung zuständigen Stellen der Finanzverwaltung sind bereits frühzeitig durch eine Verfügung der Oberfinanzdirektion Magdeburg angewiesen worden, entsprechend zu verfahren.

Der Landesbeauftragte hat mit dem MJ vereinbart, die Entwicklung weiter zu beobachten und zu gegebener Zeit den Gerichtsvollziehern im Rahmen von Zwangsvollstreckungsmaßnahmen in EDV-Anlagen entsprechende Richtlinien an die Hand zu geben.

21.7 Entwurf eines Strafverfahrensänderungsgesetzes 1994

Mit Beschluß vom 14.10.1994 wurde von den Ländern über den Bundesrat der Entwurf eines Strafverfahrensänderungsgesetzes 1994 in das Gesetzgebungsverfahren eingebracht.
Mit dem Entwurf sollen bereichsspezifische Regelungen über die Verwendung von personenbezogenen Daten, die im Strafverfahren erhoben worden sind und über ihre Verarbeitung in Dateien geschaffen sowie die Gewährleistung des Rechts auf informationelle Selbstbestimmung mit den Erfordernissen einer funktionstüchtigen Strafrechtspflege in Einklang gebracht werden. Schwerpunkte sind dabei die Regelungen über die Akteneinsicht und die Verarbeitung und Nutzung personenbezogener Informationen in Dateien der Strafrechtspflege.

Bereits mit ihrem Beschluß zur Informationsverarbeitung in Strafverfahren vom 09./10.03.1994 **(Anlage 6)** haben die Datenschutzbeauftragten des Bundes und der Länder zum vorgelegten Entwurf Stellung genommen und die Einhaltung eines datenschutzrechtlichen Mindeststandards gefordert.

Der Landesbeauftragte hat noch einmal in einer gemeinsamen Presseerklärung vom 14. Oktober 1994 den von den Ländern vorgelegten Änderungsentwurf als in weiten Teilen "unverhältnismäßige Ermächtigung zu Eingriffen in das Persönlichkeitsrecht" gerügt.
Gegenüber dem Ministerium der Justiz ist dies in einer Stellungnahme vor allem mit den vorgesehenen Regelungen in den §§ 474 und 475 des Entwurfs näher begründet worden. § 474 des Entwurfs erweitert die Akteneinsichts- und Auskunftsmöglichkeiten in Straf- und Ermittlungsakten auf fast alle öffentlichen Stellen. Damit erhalten diese personenbezogene Informationen, die teilweise nur mit den besonderen Zwangsmitteln des Strafverfahrensrechts gewonnen wurden und die sonst den anderen Stellen nach ihren gesetzlichen Eingriffsmöglichkeiten gar nicht zustehen würden.
§ 475 des Entwurfs will auch die Auskunftsmöglichkeiten für Privatpersonen erweitern und nur noch von einem berechtigten Interesse abhängig machen.

Mit diesen beiden Regelungen würden zwar die Geschäftsstellen der Strafjustizbehörden im Arbeitsumfang möglicherweise etwas entlastet, dafür würden aber die Grundrechte einer Vielzahl Betroffener (Beschuldigter oder Zeugen) mit Füßen getreten.
Es bleibt abzuwarten, wie und ob sich dieser Gesetzentwurf bei den Beratungen der Fachausschüsse des Bundestages noch entscheidend verändert.

21.8 Länderübergreifendes staatsanwaltschaftliches Verfahrensregister

Mit dem Verbrechensbekämpfungsgesetz vom 28.10.1994 wurden die gesetzlichen Grundlagen für ein bundesweites zentrales staatsanwaltschaftliches Verfahrensregister geschaffen.
Das sog. Bundes-SISY dient der Speicherung aller im Bundesgebiet anhängigen Ermittlungs- und Strafverfahren. Damit soll es den Strafverfolgungsbehörden erleichert werden, mehrere gegen eine bestimmte Person anhängige Ermittlungsverfahren zu erkennen und ggf. zusammenzufügen.

Der Landesbeauftragte hatte Gelegenheit, zu dem Entwurf der für dieses EDV-System erforderlichen Errichtungsanordnung Stellung zu nehmen. Dabei hat er vor allem auf folgende Kritikpunkte hingewiesen:

1. Die in der Errichtungsanordnung vorgesehene Datenanlieferung an das Register durch die Finanzbehörden ist von der Rechtsgrundlage des § 474 Abs. 3 StPO nicht gedeckt.

2. Soweit den Finanzbehörden Daten übermittelt werden können, hält es der Landesbeauftragte nicht für vertretbar, ihnen **alle** gespeicherten Daten zu übermitteln, weil dies in nicht wenigen Fällen dem verfassungsrechtlich begründeten Verbot der Vorratsspeicherung zuwider laufen würde. Erforderlich und zulässig ist nur eine Übermittlung personenbezogener Einzelangaben für konkrete steuerstrafrechtliche oder damit im Zusammenhang stehende Verfahren.
   Für den geplanten automatisierten Direktabruf der Finanzbehörden aus dem Register fehlt zudem die gesetzliche Grundlage.

3. Die in der Errichtungsanordnung vorgesehenen telefonischen Datenübermittlungen können nur in ganz konkret bezeichneten Ausnahmefällen zulässig sein, weil die Gefahr der Flüchtigkeit und Fehlerhaftigkeit überwiegt. Darüber hinaus dürfen die in der Errichtungsanordnung geregelten technischen und organisatorischen Schutzmaßnahmen bei einer telefonischen Datenübermittlung auch im Ausnahmefall nicht leerlaufen.

Erfolgreich hinwirken konnte der Landesbeauftragte auf eine Reduzierung der Anzahl der Personendatensätze auf das zur Identifizierung erforderliche Maß und auf eine Streichung der zunächst in der Errichtungsanordnung vorgesehenen rechtlich unzulässigen Spontanübermittlungen.

Inwieweit auch die verbliebenen Punkte noch verbessert werden können, wird vom Verlauf der noch laufenden Beratungen zwischen dem Bundesministerium der Justiz und den Landesjustizverwaltungen abhängen.

21.9 Geldwäschegesetz

Am 29.11.1993 trat das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäschegesetz) in Kraft. Das Gesetz soll der effektiven Verfolgung der Geldwäsche und damit auch der Bekämpfung der Organisierten Kriminalität dienen. Es enthält Identifizierungs- und Aufzeichnungspflichten bei Finanztransaktionen, insbesondere für Banken und andere Gewerbetreibende sowie die Verpflichtung der Meldung von Verdachtsfällen der Geldwäsche an die Strafverfolgungsbehörden.

Das Ministerium der Justiz hat unter Mitwirkung des Landesbeauftragten einen Richtlinienentwurf für die Zusammenarbeit von Staatsanwaltschaft und Polizei bei Ermittlungen im Rahmen des Geldwäschegesetzes erarbeitet, welcher im wesentlichen organisatorische Maßnahmen, die Bearbeitung von Anzeigen nach dem Geldwäschegesetz und die Bearbeitung der aufgrund von Anzeigen nach dem Geldwäschegesetz eingeleiteten Ermittlungsverfahren regelt.
Der Landesbeauftragte konnte dabei vor allem auf Regelungen zur sicheren Datenübermittlungspraxis der hochsensitiven Daten und zur Beachtung der im Geldwäschegesetz vorgeschriebenen Verwertungsverbote bezüglich der Daten

hinwirken, die im Rahmen eines Verfahrens zur Verfolgung einer Geldwäsche gewonnen wurden.

In einem Gespräch mit dem Landeskriminalamt konnte sich der Landesbeauftragte von den im wesentlichen datenschutzkonformen internen Verfahrensweisen bei der Handhabung der Bestimmungen informieren und insbesondere Hinweise zur sicheren Datenübermittlungspraxis geben.

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

Bereits in seinem I. Tätigkeitsbericht (S. 118) hat der Landesbeauftragte kritisch zu einem Entwurf zur Neufassung der RiVASt Stellung genommen. Diese Richtlinien sind für Gerichte, Staatsanwaltschaften und andere Behörden bestimmt und regeln u.a. die internationale Rechtshilfe, insbesondere die Vollstreckungshilfe und den Rechtshilfeverkehr zwischen der Polizei und den Finanzbehörden. Da der Entwurf der überarbeiteten Richtlinien an mehreren Stellen Regelungen zur Verarbeitung personenbezogener Daten enthielt, erhob der Landesbeauftragte bereits grundsätzliche Bedenken aufgrund der Tatsache, daß es sich bei den RiVASt nicht um eine gesetzliche Regelung, sondern um Verwaltungsvorschriften handelt. Eingriffe in das informationelle Selbstbestimmungsrecht des einzelnen Bürgers bedürfen aber einer gesetzlichen Regelung.

Die inhaltlichen Bedenken, die der Landesbeauftragte zu einzelnen Vorschriften der Neufassung gegenüber dem Ministerium der Justiz (MJ) ausführlich dargelegt hat und die auch vom Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Justiz (BMJ) deutlich gemacht wurden, fanden jedoch keinen Niederschlag in den Beratungen von Bund und Ländern. Die Bundesregierung und die Länderregierungen vereinbarten die Neufassung der RiVASt in einer im Vergleich zum Entwurf nahezu unveränderten Fassung. Sie wurden mit Verfügung des MJ zum 01.03.1993 für das Land Sachsen-Anhalt in Kraft gesetzt.
Damit fehlt in diesem Bereich jedenfalls die von der Verfassung geforderte **gesetzliche** Grundlage. Das MJ bleibt deshalb aufgefordert, sich beim BMJ für

eine entsprechende unverzügliche Überarbeitung des Gesetzes über die internationale Rechtshilfe in Strafsachen einzusetzen, damit darin die erforderlichen Regelungen getroffen werden.

21.11 Überprüfung der Staatsanwaltschaften

Im Berichtszeitraum hat der Landesbeauftragte begonnen, schwerpunktmäßig bei den Staatsanwaltschaften insbesondere die datenschutzgerechte Führung der Zentralen Namenskartei, die Rückmeldungen der Staatsanwaltschaften an die Polizei über die Ergebnisse der Ermittlungsverfahren und die Aufbewahrung von Beweismitteln nach Verfahrenseinstellungen sowie die technischen und organisatorischen Regelungen zur Sicherheit der dort aufbewahrten personenbezogenen Daten zu überprüfen.

1. Bei der Überprüfung des Rückmeldeverfahrens zum Ausgang der staatsanwaltschaftlichen Ermittlungen an die Polizei mußte der Landesbeauftragte feststellen, daß dieses nicht in jedem Falle gewährleistet ist. Die Gründe dafür lagen in organisatorischen Mängeln, weil das entsprechende Formular der Polizei nicht in jedem Fall in der Ermittlungsakte war. Da es auch bei den Staatsanwaltschaften nicht vorgehalten wurde, unterblieb in diesen Fällen eine Rückmeldung an die Polizei.
   Der Landesbeauftragte hat in diesem Zusammenhang darauf hingewiesen, daß es zur ordnungsgemäßen Erfüllung der polizeilichen Aufgaben erforderlich ist, daß die bearbeitenden Polizeidienststellen über das Ergebnis der staatsanwaltschaftlichen Ermittlungsverfahren unterrichtet sind.
   Die Empfehlung des Landesbeauftragten, entsprechende Vordrucke bei den Staatsanwaltschaften zur Ergänzung vorzuhalten, wurde bei den betroffenen Staatsanwaltschaften inzwischen umgesetzt.

2. Im Rahmen seiner Überprüfung stieß der Landesbeauftragte wiederholt auf alte Karteikarten, die von den ehemaligen Kreis- und Bezirksstaatsanwaltschaften der DDR auch zur Aktenverwaltung angelegt wurden. Die Karteikarten enthielten Hinweise auf Ermittlungsverfahren, die nach den heutigen Rechtsvorschriften nicht mehr eingeleitet werden dürfen (z.B. Republikflucht, Verleumdung von Staatsorganen, asoziales Verhalten), aber auch auf Be-

schwerden, über Entscheidungen der betrieblichen Konfliktkommissionen oder auch über Untätigkeiten der Staatsanwaltschaften. Die dazugehörenden Akten konnten entweder nicht oder nur noch teilweise und im ungeordneten Zustand aufgefunden werden.

Die aufgefundenen Karteikarten sind unter Berücksichtigung eines Erlasses des Ministeriums der Justiz (MJ) vom 19.04.1993 bislang nicht vernichtet worden. Die im Erlaß enthaltenen Aufbewahrungsbestimmungen sind unter Berücksichtigung der §§ 34 und 36 DSG-LSA zum Teil nicht rechtskonform. Die aufbewahrten Karteikarten hätten unter Berücksichtigung der §§ 34, 36 DSG-LSA zumindest gesperrt werden müssen, soweit sie nicht nach den Bestimmungen des Einigungsvertrages zu löschen waren.
Seitens des MJ wurde inzwischen eine Überarbeitung des entsprechenden Erlasses vorgelegt, nach der die entsprechenden Unterlagen, einschließlich der Karteikarten der Staatsanwaltschaften der ehemaligen DDR, zu sperren sind und nur gem. § 16 Abs. 5 DSG-LSA genutzt werden dürfen (z.B. zum Zwecke von Rehabilitierungsverfahren oder zur Strafverfolgung von SED-Unrecht).

3. Im Rahmen der stichprobenhaften Überprüfung der Ermittlungsakten wurde festgestellt, daß in einer Reihe von Fällen zwar die eigentlichen Ermittlungsakten des MfS an den Bundesbeauftragten für die Stasi-Unterlagen abgegeben worden waren, daß aber die dazu gehörenden Handakten sich teilweise noch in den Geschäftsstellen der Staatsanwaltschaften befanden. Diese nach altem Recht angelegten Handakten enthalten auch diverse Originalunterlagen.
   Der Landesbeauftragte hat deshalb darauf hingewiesen, daß nach § 8 Abs. 1 StUG **alle** Akten dem Bundesbeauftragten zuzuleiten sind. Nur so kann sichergestellt werden, daß die Akten beim Bundesbeauftragten vollständig vorhanden sind und im Rahmen des gesetzlichen Auftrags entsprechend genutzt werden können.

4. Bei einem Teil der überprüften Staatsanwaltschaften war bereits das automatisierte Geschäftsstellenbearbeitungssystem SIJUS-Strafsachen zur automatischen Erfassung aller vorhandenen Ermittlungsakten eingeführt.

Dieses Verfahren ist auf die neu anzulegenden Ermittlungsakten beschränkt. Bereits früher angelegte Akten werden weiter konventionell bearbeitet.
Bei der Eingangserfassung im SIJUS-System werden die persönlichen Daten der Beschuldigten und bei qualifizierten Sachen mit unbekannten Tätern sowie bei Tötungs- und Selbsttötungsdelikten die Daten der Opfer gespeichert, unabhängig vom Alter und der Schuldfähigkeit. Darüber hinaus enthielt die Bildschirmmaske zur Erfassung als auszufüllendes Datum auch den Namen der Mutter des Betroffenen.
Bereits in seinem I. Tätigkeitsbericht (S. 131) hatte der Landesbeauftragte darauf hingewiesen, daß für den Einsatz des SIJUS-Verfahrens zur Zeit keine ausreichende rechtliche Grundlage besteht. Auch wenn es im Hinblick auf die besondere Situation in Sachsen-Anhalt und das Erfordernis einer schnellen und organisatorisch unkomplizierten Arbeitsweise der sich noch im Aufbau befindlichen Staatsanwaltschaften nach Auffassung des Landesbeauftragten für eine Übergangsphase hinnehmbar ist, die Auffangregelungen im DSG-LSA mit den von der Rechtsprechung für diese Fälle herausgearbeiteten Einschränkungen anzuwenden, um zumindest einen gewissen datenschutzrechtlichen Mindeststandard zu gewährleisten, darf bis zur Schaffung einer entsprechenden bundesgesetzlichen Rechtsgrundlage in dieser Übergangsphase nur das zur Aufgabenerledigung unbedingt "Erforderliche" gespeichert und verarbeitet werden.

Gemessen an diesem Maßstab ist die Erhebung und Speicherung des Namens der Mutter des Betroffenen nicht erforderlich.
Auf den entsprechenden Hinweis des Landesbeauftragten wurde von den betroffenen Staatsanwaltschaften der Name der Mutter nicht mehr in die SIJUS-Dateien eingestellt.

Bei der technischen Überprüfung des SIJUS-Systems durch den Landesbeauftragten wurden datenschutzrechtliche Mängel des eingesetzten Programms deutlich. Hierzu gehört der Umstand, daß nach einer Dateneingabe eine Löschung dieser Datenfelder als Programmfunktion nicht mehr durchführbar ist. Hilfsweise ist nur ein Überschreiben der Feldinhalte möglich.

Auch eine automatische Löschfristenüberwachung ist nicht vorhanden. Damit besteht einerseits die Gefahr einer zu langen Speicherung nicht mehr erforderlicher Daten, andererseits wird die gesetzlich in § 16 Abs. 2 DSG-LSA (als Übergangsregelung) vorgeschriebene Löschung nur mit einem zusätzlichen Aufwand möglich.

21.12 Fehlerhafter Umgang mit Altdatenbeständen bei einer Staatsanwaltschaft

Aus verschiedenen Presseberichten erfuhr der Landesbeauftragte davon, daß im Zusammenhang mit Umzugsmaßnahmen einer Staatsanwaltschaft alte personenbezogene Aktenbestände (Anklageschriften und Urteile) unbeaufsichtigt in einem offenen Container auf öffentlicher Straße gelagert wurden, so daß sich unbefugte Personen die personenbezogenen Unterlagen verschaffen, von deren Inhalt Kenntnis nehmen und teilweise auch der Presse übergeben konnten.

Der Landesbeauftragte hat diesen Vorgang überprüft und, nachdem sich der Sachverhalt bestätigt hat, gegenüber dem Ministerium der Justiz (MJ) gem. § 24 Abs. 1 Satz 1 DSG-LSA eine förmliche Beanstandung der Verletzung datenschutzrechtlicher Vorschriften ausgesprochen.

Die Staatsanwaltschaft war für die in Rede stehenden personenbezogenen Unterlagen speichernde Stelle (§ 2 Abs. 8 DSG-LSA). Ihr oblag daher die Pflicht, durch geeignete technische und organisatorische Maßnahmen sicherzustellen, daß die bei ihr gelagerten personenbezogenen Daten in jeder der gesetzlich definierten Verarbeitungsphasen (vgl. § 2 Abs. 5 DSG-LSA) ausreichend geschützt waren, insbesondere nicht unbeaufsichtigt blieben und nicht unbefugt zur Kenntnis Dritter gelangten (§ 5 DSG-LSA). Diese Verantwortung wurde zwar von der Staatsanwaltschaft gesehen und anerkannt, jedoch wurde sie nicht mit der notwendigen Gewissenhaftigkeit bei den vorgenommenen Umzugs- und Entsorgungsarbeiten umgesetzt.

Der Landesbeauftragte hält die vom MJ in seiner Stellungnahme zur Beanstandung mitgeteilten Maßnahmen für geeignet und ausreichend, um dort künftig den erforderlichen Schutz personenbezogener Daten sicherzustellen.

21.13 Übermittlungsersuchen des Verfassungsschutzes an Staatsanwaltschaften

Gemäß § 18 Abs. 3 BVerfSchG können das Bundesamt für Verfassungsschutz und nach § 17 Abs. 3 VerfSchG-LSA das Landesamt für Verfassungsschutz des Landes Sachsen-Anhalt an die Staatsanwaltschaften Übermittlungsersuchen richten.

Diese Ersuchen sind nach dem strafprozessualen Grundsatz der Aktenvollständigkeit in den Akten der Staatsanwaltschaft aufzubewahren. Unter dem Gesichtspunkt des nachrichtendienstlich sensiblen Hintergrundes eines Ersuchens stellte sich die Frage, ob diese Schreiben in die staatsanwaltschaftlichen Sachakten oder in den Handakten abzuheften sind. Beim Abheften in der Sachakte wäre das Ersuchen für einen nicht überschaubaren Kreis von Personen bei Akteneinsichten zugänglich gewesen.

Der Landesbeauftragte hat daher dem Ministerium der Justiz (MJ) empfohlen, eine Regelung dahingehend zu treffen, daß Übermittlungsersuchen der Verfassungsschutzbehörden an die Staatsanwaltschaften und deren entsprechende Verfügungen grundsätzlich nur in den intern verwendeten und Dritten nicht zugänglichen Unterlagen (Handakten) aktenkundig zu machen sind. Die Schriftstücke sollten jedoch dann zu den Sachakten genommen werden, sofern sich daraus be- oder entlastende Hinweise für den Beschuldigten ergeben, die für das Ermittlungsverfahren oder für die gerichtliche Entscheidung von Bedeutung sein können.

Unter Hinweis auf die verfassungsrechtlich gebotene Pflicht zum grundsätzlich offenen Umgang staatlicher Stellen mit dem Bürger und unter dem Gesichtspunkt der Gewährung eines effektiven Rechtsschutzes des Betroffenen hat der Landesbeauftragte darüber hinaus darauf hingewiesen, daß bei einem Akteneinsichtsgesuch des Betroffenen im Regelfall von Amts wegen auf den vorhandenen Schriftwechsel mit den Verfassungsschutzbehörden hinzuweisen ist, ggf nach vorheriger Beteiligung der Verfassungsschutzbehörden.

Das MJ hat beide Empfehlungen des Landesbeauftragten in einem Runderlaß vom 13.07.1994 umgesetzt.

21.14 Übermittlung/Weitergabe von Vorstrafen bei Vernehmungen

Aufgrund der Eingabe eines Bürgers hatte der Landesbeauftragte dazu Stellung zu nehmen, inwieweit es nach der StPO zulässig ist, bei Zeugen- und Beschuldigtenvernehmungen durch die Polizei die Vorstrafen eines Beschuldigten den Zeugen oder anderen Beschuldigten durch Verlesen zur Kenntnis zu geben.

Gemäß §§ 161 und 163 StPO haben die Beamten des Polizeidienstes Straftaten zu erforschen und auf Weisung der Staatsanwaltschaft jede Art von Ermittlungen vorzunehmen. Soweit in solchen Fällen personenbezogene Daten übermittelt werden, ist die rechtliche Beurteilung strittig.
In der Literatur und in vereinzelten Gerichtsentscheidungen wird die Auffassung vertreten, die genannten Rechtsvorschriften der StPO stellten eine hinreichende Rechtsgrundlage für die Übermittlung von Daten an Dritte im Zuge der strafrechtlichen Ermittlungen dar.
Der Landesbeauftragte folgt in Übereinstimmung mit den Datenschutzbeauftragten des Bundes und der Länder dieser Auffassung nicht, sondern verlangt dazu seit langem vom Bundesgesetzgeber ergänzende klare Regelungen in der StPO, um den verfassungsrechtlichen Anforderungen gerecht zu werden. Für eine Übergangszeit werden die Datenschutzgesetze für ergänzend anwendbar gehalten.

Nach § 12 Abs. 1 Nr. 1 DSG-LSA ist danach im Einzelfall eine Datenübermittlung in den privaten Bereich nur zulässig, wenn es zur Aufgabenerfüllung erforderlich ist und die Voraussetzungen des § 10 DSG-LSA eine Nutzung zulassen. Anwendbar war hier § 10 Abs. 2 Nr. 7 DSG-LSA, der die Übermittlung zur Verfolgung von Straftaten zuläßt. Neben der Prüfung der Tatbestandsmäßigkeit einer strafbaren Handlung gehören dazu nach der Rechtsprechung auch die Feststellung der Schuldform sowie die Beantwortung der Frage, inwieweit ein Unrechtsbewußtsein bei dem Beschuldigten vorgelegen hat. In diesem Zusammenhang war es nach Auffassung des Landesbeauftragten im vorliegenden Einzelfall jedenfalls vertretbar, wenn die vernehmenden Polizeibeamten herauszufinden versucht haben, ob, und wenn ja, welche Vorstrafen der anderen Beteiligten den jeweils Beschuldigten bekannt waren. Dieses Wissen hatte zudem bei den

im konkreten Fall in Frage kommenden Delikten aus dem Bereich der Korruptionskriminalität auch für die spätere Strafzumessung eine erhebliche Bedeutung und war insoweit auch erforderlich im Sinne der genannten Vorschriften.

21.15 Aktenaufbewahrung nach Einstellung des Strafverfahrens

Ein Bürger wandte sich mit der Bitte um Prüfung an den Landesbeauftragten, inwieweit eine weitere Datenspeicherung nach Einstellung eines Strafverfahrens noch zulässig ist.

Gemäß § 160 StPO ist es Aufgabe der Staatsanwaltschaft, Ermittlungsverfahren durchzuführen. Dieses Recht schließt nach höchstrichterlicher Rechtsprechung das Recht und die Pflicht zur Führung von Akten mit ein, ohne daß dies im Gesetz ausdrücklich angesprochen sein muß. Die Aktenführung kann auch im Interesse des betroffenen Bürgers liegen, weil sie z.B. auch Nachweise zu seinen Gunsten ermöglicht.

Allerdings bedarf die Speicherung personenbezogener Daten in Akten und Dateien der Staatsanwaltschaften nach Auffassung des Landesbeauftragten einer speziellen gesetzlichen Regelung. § 160 StPO reicht dazu nicht mehr aus. Die Vorschrift erfüllt nicht die vom Bundesverfassungsgericht aufgestellten Anforderungen an Normenklarheit und Bestimmtheit des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung.

Obwohl die Datenschutzbeauftragten des Bundes und der Länder seit Jahren beim dafür zuständigen Bundesgesetzgeber auf die Notwendigkeit einer datenschutzkonformen gesetzlichen Regelung hingewiesen haben, fehlt diese Regelung noch immer. Der Gesetzgeber beruft sich, unterstützt von der Rechtsprechung, zur Zeit immer noch auf eine Übergangsfrist.

Für diese Übergangszeit gilt als Rechtsgrundlage im Land Sachsen-Anhalt das DSG-LSA. Nach § 16 Abs. 2 Nr. 2 DSG-LSA sind die Daten (erst) zu löschen, wenn deren Kenntnis für die Staatsanwaltschaft zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist.

Die im vorliegenden Fall nach § 153 StPO vorgenommene Einstellung des Verfahrens mit Zustimmung des Amtsgerichts bedeutet, daß ein - geringer - Schuldvorwurf vorlag und erhalten blieb. In solchen Fällen ist es zulässig, die entsprechenden Einspeicherungen bzw. die Ermittlungsakte mit einer Aufbewahrungsfrist zu belegen, u.a. damit der Betroffene gewarnt ist; im Wiederholungsfall muß er mit der Einbeziehung des alten Falles zumindest in die Bewertung rechnen.

21.16 Eintragung der Schuldfähigkeit in das Bundeszentralregister

Gemäß § 11 Abs. 1 Ziff. 1 BZRG ist in bestimmten Fällen durch die zuständige Staatsanwaltschaft eine Meldung an das Bundeszentralregister vorzunehmen, wenn ein Verfahren wegen erwiesener oder nicht auszuschließender Schuldunfähigkeit etc. abgeschlossen wurde. Der Beschuldigte wird aber über eine Verfahrenseinstellung nur unterrichtet, wenn er als solcher vernommen worden ist, ein Haftbefehl gegen ihn erlassen war oder er um einen Bescheid gebeten hat bzw. ein besonderes Interesse an der Bekanntgabe ersichtlich ist. In den übrigen Fällen erfährt er auch nicht, daß im Rahmen des § 11 BZRG eine entsprechende Meldung über ihn erfolgt.

Diese Verfahrensweise berücksichtigt nicht das verfassungsmäßig garantierte Recht auf informationelle Selbstbestimmung, das in Sachsen-Anhalt ausdrücklich in Art. 6 Abs. 1 der Verfassung festgelegt wurde.
Der Landesbeauftragte hat daher gegenüber dem Ministerium der Justiz (MJ) angeregt, daß die zuständigen Staatsanwaltschaften des Landes den Beschuldigten über die Eintragung der Einstellung des Verfahrens wegen Schuldunfähigkeit im Bundeszentralregister belehren, damit dieser weiß, wann und wo seine personenbezogenen Daten gespeichert werden.

Das MJ hat diese Anregung aufgegriffen und im Rahmen einer Verwaltungsvorschrift vom 14.12.1993 die Unterrichtung des Beschuldigten über eine Eintragung nach § 11 Abs. 1 Nr. 1 BZRG vorgeschrieben.

21.17 Datenübermittlung beim Täter-Opfer-Ausgleich

Der Landesverband für Straffälligen- und Bewährungshilfe Sachsen-Anhalt e.V. ist mit der Bitte an den Landesbeauftragten herangetreten, im Rahmen einer Fortbildungsveranstaltung zu Fragen der Datenübermittlung an den Verein bzw. dessen Mitglieder durch Gerichte und Staatsanwaltschaften bei der Durchführung des Täter-Opfer-Ausgleiches Stellung zu nehmen. Mit dem Verfahren wird versucht, eine persönliche Verbindung zwischen Täter und Opfer einer Straftat unter Vermittlung eines dafür geschulten Dritten herzustellen und den dabei angerichteten immateriellen und materiellen Schaden so gut es geht zu beheben.

Der Landesbeauftragte mußte dazu auf die Rechtslage verweisen, wonach zur Durchführung des Täter-Opfer-Ausgleiches mangels Regelung im Bundesrecht eine Datenübermittlungsmöglichkeit ohne vorherige Einwilligung beider Betroffener nur übergangsweise auf der Grundlage des DSG-LSA und nur im Zusammenhang mit Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes besteht. Gericht und Staatsanwalt können in diesen Fällen an den Sozialen Dienst der Justiz, aber auch an einen privaten Verein für Straffälligen- und Bewährungshilfe personenbezogene Angaben zur Person des Täters und des Opfers aus ihren Akten für einen solchen Vermittlungs- bzw. Ausgleichsversuch übermitteln (§ 11 Abs. 1 bzw. § 12 Abs. 1 Nr. 1 i.V. mit § 10 Abs. 2 Nr. 7 DSG-LSA).

Jedoch sollte auch hierbei vor einer Datenübermittlung, nach dem Grundsatz der primären Datenerhebung bei dem Betroffenen (§ 9 Abs. 2 Satz 1 DSG-LSA), zunächst die Einwilligung der betroffenen Personen eingeholt werden.

Im Erwachsenenstrafrecht hingegen ist auch über das DSG-LSA keine Datenübermittlung von Amts wegen möglich, da trotz des deutlichen Hinweises der Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren zu § 46a StGB weder im StGB noch in der StPO eine gesetzliche Grundlage zur Datenübermittlung zur Durchführung des Täter-Opfer-Ausgleiches vorgesehen wurde.

Die Datenübermittlung (z.B. Namen und Anschriften) durch die Justiz an vermittelnde Stellen ist in diesen Fällen nur nach vorheriger Einwilligung der jeweils Betroffenen (Täter und Opfer) zulässig. Dabei ist § 4 Abs. 2 DSG-LSA zu beachten.

21.18 Praktika von Jurastudenten bei der Polizei

An den Landesbeauftragten ist mehrfach die Frage herangetragen worden, inwieweit Jurastudenten am praktischen Polizeidienst teilnehmen können.

Die Ausbildungs- und Prüfungsordnung für Juristen in Sachsen-Anhalt vom 01.02.1993 sieht in § 11 Abs. 4 eine praktische Studienzeit bei einem Amtsgericht vor, bei der u.a. eine anschauliche Vorstellung von der Arbeit eines Staatsanwalts vermittelt werden soll. Bei der Durchführung dieses Praktikums ist auch nicht auszuschließen, daß den Studenten die Zusammenarbeit der Staatsanwaltschaft mit ihren Hilfsbeamten, bei der Polizei, dargestellt werden soll.

Der Landesbeauftragte hat gegenüber der Generalstaatsanwaltschaft darauf hingewiesen, daß bei diesen Praktika Vorsicht geboten ist, wenn es im Zuge ihrer Durchführung zu Übermittlungen personenbezogener Daten an die Praktikanten kommt. Zwar wäre es aus datenschutzrechtlicher Sicht am einfachsten, Jurastudenten während ihrer Praktikantenzeit, z.B. in einer Polizeidienststelle oder bei der Teilnahme am Streifendienst der Polizei, nur mit Daten in Verbindung zu bringen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen, jedoch wird sich das in der Praxis weder einhalten lassen noch ist dies immer mit einer realistischen Arbeitsweise in Einklang zu bringen.

Von daher begrüßt es der Landesbeauftragte ausdrücklich, daß nach Mitteilung der Generalstaatsanwaltschaft bei den künftig vorgesehenen Praktika die Jurastudenten einer besonderen Belehrung und Verpflichtung nach dem Verpflichtungsgesetz auf das Datengeheimnis unterzogen werden sollen.

21.19 Verwendung von Justizakten zu Studien- und Prüfungszwecken

Bereits in seinem I. Tätigkeitsbericht (S. 124) hatte der Landesbeauftragte gefordert, die Verwendung von Originalakten der Justiz zu Prüfungszwecken gesetzlich zu regeln. Eine solche Regelung war vor allem deswegen geboten, weil es sich bei dieser Verwendung um eine Zweckänderung und mithin um einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen handelt. Denn die Daten sind ursprünglich erhoben und gespeichert worden, um den entsprechenden Verwaltungsvorgang zu bearbeiten oder eine gerichtliche Entscheidung herbeizuführen, und nur dafür haben die Betroffenen sie herausgegeben.

Anfang 1994 legte die Landesregierung den Entwurf eines Gesetzes über die Juristenausbildung im Land Sachsen-Anhalt vor und der Landesbeauftragte hatte Gelegenheit zur Stellungnahme. Dabei griff er sein weiteres Anliegen auf, alle Prüfungsakten nach Möglichkeit zu anonymisieren. Die Landesregierung wollte dies so wegen des Verwaltungsaufwandes nicht für alle Fälle übernehmen. Im Ergebnis wurde ein Kompromiß erreicht, der vorsieht, daß den Rechtsreferendaren Gerichts- und Verwaltungsakten zur Bearbeitung übergeben werden können, soweit nicht im Einzelfall andere gesetzliche Vorschriften oder überwiegende schutzwürdige Belange Betroffener einer Übermittlung der personenbezogenen Daten entgegenstehen. Das Landesjustizprüfungsamt muß dann im konkreten Fall entscheiden, ob es in einem solchen Fall von der Ausgabe der Akten zu Prüfungszwecken absehen oder eher anonymisieren will.

Dieser Vorschlag ist aufgegriffen worden und in § 2 Abs. 5 des Juristenausbildungsgesetzes vom 27.04.1994 Gesetz geworden.

22. Öffentlich-rechtliche Religionsgesellschaften

Öffentlich-rechtliche Religionsgesellschaften verarbeiten eine Fülle personenbezogener Daten ihrer Mitglieder. Derartige Daten erhalten sie häufig von staatlichen Stellen, so daß sich der Datenschutz bei den öffentlich-rechtlichen

Religionsgesellschaften an dem Maßstab des vom Staat gewährten Schutzes orientieren muß.

Nach § 11 Abs. 4 DSG-LSA dürfen öffentliche Stellen des Landes an öffentlich-rechtliche Religionsgesellschaften personenbezogene Daten übermitteln, wenn dort ausreichende Datenschutzmaßnahmen getroffen worden sind. Die entsprechende Feststellung hierzu hat das Ministerium des Innern durch den Runderlaß vom 17.08.1993 (MBl. LSA S. 2105) getroffen.
Die gesetzliche Regelung, wonach sichergestellt sein muß, daß die Datenschutzmaßnahmen denen des Staates gleichwertig sind, hat z.B. praktische Bedeutung im Melderecht, weil nach § 30 MG LSA die Meldebehörde der öffentlich-rechtlichen Religionsgesellschaft zur Erfüllung ihrer Aufgaben Daten ihrer Mitglieder aus dem Melderegister übermitteln darf.

Inzwischen hat die Evangelische Kirche in Deutschland ihr Kirchengesetz über den Datenschutz vom 12. November 1993 veröffentlicht. Auch bei der Katholischen Kirche ist am 1. Januar 1994 die "Anordnung über den kirchlichen Datenschutz" - KDO - in Kraft gesetzt worden.
Damit verfügen die beiden großen Kirchen über ein zeitgemäßes Datenschutzrecht, das sich am Standard des Bundesdatenschutzgesetzes orientiert.

23. Öffentlich-rechtliche Rundfunkanstalten

23.1 Die Fahndung nach Schwarzhörern und -sehern

Die öffentlich-rechtlichen Rundfunkanstalten betreiben gemeinsam die Gebühreneinzugszentrale (GEZ) in Köln. Diese prüft - im Auftrag der jeweiligen Landesrundfunkanstalt -, ob Rundfunk- und Fernsehgeräte ordnungsgemäß angemeldet sind und die Gebühren bezahlt wurden. Dazu bedient sie sich eigener Mitarbeiter, die von Haus zu Haus gehen, oder holt Einzelauskünfte beim zuständigen Einwohnermeldeamt nach § 33 MG LSA ein. Dieses Auskunftsverfahren ist aus datenschutzrechtlicher Sicht nicht zu beanstanden.

1993 hatten die Rundfunkanstalten eine neue Idee, um ihrer Meinung nach Schwarzhörer und -seher besser aufspüren zu können. Es sollte eine regelmäßige Datenübermittlung zwischen allen Einwohnermeldeämtern in der Bundesrepublik und der GEZ geben. Dazu sollten, ohne daß die an sich zuständigen Länderparlamente und die Bürger etwas merkten, die Meldebehörden durch eine kleine Ergänzung der Meldedatenübermittlungsverordnungen der Länder verpflichtet werden, jeden Fall der Anmeldung, Abmeldung, Ummeldung oder des Todes eines volljährigen Einwohners zu melden. Dabei sollten der Name, Doktorgrad, Geburtstag, gegenwärtige und frühere Anschriften, Tag des Ein- und Auszuges, Familienstand und im Todesfall den Sterbetag der GEZ übermittelt werden.

Eine solche Regelung würde in mehrfacher Weise gegen das Grundgesetz und die Landesverfassung in Sachsen-Anhalt verstoßen.
Verletzt würde in rechtswidriger Weise nicht nur das Grundrecht auf informationelle Selbstbestimmung einer Vielzahl betroffener Bürger, sondern es käme in der praktischen Anwendung bei der GEZ zu einem - verfassungswidrigen - bundesweiten "Melde"-Register und zur verfassungsrechtlich unzulässigen Überschreitung der den Landesrundfunkanstalten gezogenen Ländergrenzen. **Jede** Rundfunkanstalt hätte einen unkontrollierten Zugriff auf **alle** darin gespeicherten personenbezogenen Daten **aller** Bürger, ganz gleich, ob sich der Bürger im Zuständigkeitsbereich der Anstalt befindet und bei ihr gebührenpflichtig ist oder nicht.
Bei diesem Verfahren bliebe rechtlich unbeachtet, ob überhaupt eine Gebührenpflicht des betroffenen Bürgers besteht - und damit eine Rechtsgrundlage nach § 4 des Rundfunkgebührenstaatsvertrages -, oder ob der betroffene Bürger bereits von sich aus seiner Anzeigepflicht nach § 3 des Rundfunkgebührenstaatsvertrages längst nachgekommen ist und damit seitens der GEZ gegen das Verbot der Doppelerhebung verstoßen würde.
Verstoßen würde bei der vorgesehenen Pauschalübermittlung in Sachsen-Anhalt auch gegen § 32 MG LSA. Regelmäßige Datenübermittlungen dürfen nach dieser Vorschrift nur dann erfolgen, wenn sie zur Erfüllung der in der Zuständigkeit der Empfänger liegenden Aufgaben erforderlich sind. Gerade dies ist z.B. bei den Personen, die kein Fernseh- oder Rundfunkgerät zum Empfang bereithalten, und all den Bürgern, die ihre Gebühren bezahlt haben, nicht der Fall. Eine solche Verordnung würde damit auch gegen den Grundsatz der Verhältnismäßigkeit verstoßen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb auf Vorschlag des Landesbeauftragten in einem Beschluß vom 26./27. Oktober 1993 die regelmäßige Datenübermittlung von Meldedaten an die öffentlich-rechtlichen Rundfunkanstalten (gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens) abgelehnt **(Anlage 2).**

23.2 Befreiung von der Rundfunkgebührenpflicht aus sozialen Gründen

Der seit 1992 auch in Sachsen-Anhalt gültige Rundfunkgebührenstaatsvertrag der Länder sieht in § 6 die Möglichkeit vor, daß die Landesregierung durch eine Verordnung bestimmte Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht regeln kann. Das hat die Landesregierung inzwischen getan, und so ist es für bedürftige Bürger möglich, einen Antrag auf Gebührenbefreiung aus sozialen Gründen zu stellen. Der Antrag wird zwar beim zuständigen Sozialamt entgegengenommen, das Amt darf aber über den Antrag nicht abschließend entscheiden, sondern schickt nach eigener Prüfung nur einen Vorschlag an die Landesrundfunkanstalt. Der auch für Sachsen-Anhalt zuständige MDR hat in seinem dazu ergangenen Rundschreiben an die Sozialämter darum gebeten, mit dem Vorschlag auch kopierte Belege und Nachweise zur sozialen Bedürftigkeit zu übersenden.

Diese Verfahrensweise halten die Landesbeauftragten Sachsens, Thüringens und Sachsen-Anhalts für bedenklich, weil die Sozialämter nicht ohne weiteres berechtigt sind, ohne Einwilligung des Betroffenen dessen sensitive Einzeldaten an den MDR bzw. der Gebühreneinzugszentrale (GEZ) zu übersenden. Auch wenn nicht in jedem Fall die engen Voraussetzungen des § 35 SGB I (Sozialgeheimnis) gegeben sind, soll doch der den Sozialämtern besonders vertraute Schutzgedanke bei dieser Verfahrensweise einfließen.

Wenn aber **alle** Unterlagen des Betroffenen an den MDR weitergeleitet werden müssen, bleibt die bisherige rechtliche Mitwirkung der Sozialämter ohne rechtliche Bedeutung, und es findet dort nur eine überflüssige Datenerhebung und -verarbeitung statt. Es erscheint dann aus datenschutzrechtlicher Sicht nur

konsequent, die Bearbeitung von vornherein ausschließlich dem MDR zu übertragen. Das schließt nicht aus, daß der Betroffene seinen Antrag ortsnah beim Sozialamt abgeben kann und er von dort unverzüglich ohne eigene inhaltliche Prüfung an den MDR weitergeleitet wird.

Da eine solche Umgestaltung des bisherigen Verfahrens direkt den Aufgabenkreis der Landkreise und kreisfreien Städte berührt, hat das vom Landesbeauftragten um Stellungnahme gebetene Ministerium für Arbeit, Soziales und Gesundheit zunächst den kommunalen Spitzenverbänden Gelegenheit zur Abgabe ihres Votums gegeben. Diese teilen im wesentlichen die Auffassung des Landesbeauftragten, so daß eine Chance besteht, nicht erforderliche Datenflüsse und -sammlungen einzudämmen.

24. Schulen

24.1 Regelungen zum Datenschutz im Schulgesetz

Das Schulreformgesetz für das Landes Sachsen-Anhalt (Vorschaltgesetz) vom 11.07.1991 war bis zum 31.12.1992 zu novellieren. Datenschutzrechtliche Regelungen waren im Vorschaltgesetz nicht vorhanden. Deshalb hatte der Landesbeauftragte frühzeitig beim Kultusministerium darauf gedrungen, bereichsspezifische datenschutzrechtliche Regelungen mit aufzunehmen. Nachahmenswerte Vorbilder gab es im Hessischen Schulgesetz, aber auch in den erläuternden Hinweisen für die Schule zum Vollzug des Bayerisches Datenschutzgesetzes vom 03.03.1989.

Die Chance wurde nicht genutzt, und die Forderungen des Landesbeauftragten wurden ein Opfer der Eile des Gesetzgebers. Nur in einem einzigen Paragraphen der Neufassung des Schulgesetzes (§ 84a) gibt es jetzt eine generalklauselartige Regelung zur Datenverarbeitung in Schulen und den rund um die Schule beteiligten öffentlichen Stellen sowie eine Regelung über das Recht auf Auskunft, Einsicht, Beteiligung, Sperrung oder Löschung von Daten. Im übrigen wird auf die Bestimmungen des DSG-LSA verwiesen.

Der Landesbeauftragte hält schon deshalb eine Ergänzung dieser Bestimmungen im Schulgesetz für erforderlich, weil bisher Regelungen zur Datenerhebung fehlen und weil gerade die Schule mit vielen zigtausend Betroffenen (Schüler, Eltern, Lehrer) mit gutem Beispiel vorangehen sollte, wenn es darum geht, den Umgang mit den persönlichen Rechten des einzelnen richtig bewerten und gestalten zu lernen.

24.2 Datenschutz im Berufsschulwesen

Petenten einer Berufsbildenden Schule wandten sich an den Landesbeauftragten mit der Bitte, folgende Sachverhalte datenschutzrechtlich zu bewerten:

1. Dürfen Fehlstunden aus datenschutzrechtlichen Gründen auf einem Zeugnis aufgeführt werden?
2. Dürfen Informationen über Fehlzeiten in Form von Listen an die zuständige Innung weitergereicht werden?
3. Dürfen neben den üblichen Anwesenheitslisten zusätzliche Personenkontrollkarten geführt werden?

Die um Stellungnahme gebetene Schulleitung rechtfertigte ihr bisheriges Vorgehen damit, daß in vielen Fällen sowohl die Pünktlichkeit als auch die Regelmäßigkeit des Schulbesuches zu wünschen übrig lassen. Sie wies darauf hin, daß die Personenkontrollkarten eine Maßnahme der Innung darstellte, die von den unterrichtenden Lehrkräften wohlwollend unterstützt wurde. Des weiteren teilte sie dem Landesbeauftragten mit, daß die betreffende Innung beabsichtige, die Personenkontrollkarten landesweit einzuführen. Von der Schule selbst wurden zur Kontrolle Anwesenheitslisten geführt.

Die datenschutzrechtliche Prüfung zu den einzelnen Problembereichen hat folgendes ergeben:

1. Nach § 84a Abs. 3 des Schulgesetz dürfen die Schulen personenbezogene Daten der Schülerinnen und Schüler verarbeiten (hierzu gehören auch Eintragungen auf dem Zeugnisformular über Fehlzeiten), soweit dieses u.a. zur Erfüllung des Erziehungs- und Bildungsauftrages erforderlich ist.

Was im einzelnen dazu gehört, ergibt sich aus dem Schulgesetz. Das Schulgesetz regelt die Pflicht der Schulen zur umfassenden allgemeinen und beruflichen Ausbildung und die Pflichten der Schüler zur regelmäßigen Teilnahme am Unterricht. Der Kultusminister, als oberste Fachinstanz, durfte diese gesetzlichen Anforderung praxisnah interpretieren und für die Schulen bindend regeln.
Dies hat er durch Erlaß vom 10.01.1994 getan. Nach Ziff. 4.4 des Erlasses sind Unterrichtsversäumnisse auf dem Zeugnis einzutragen. Ausnahmen sind nur für Abgangszeugnisse und Abschlußzeugnisse vorgesehen.

Die Angaben zu Unterrichtsversäumnissen während der laufenden Schulpflicht geben wichtige Anhaltspunkte sowohl zur Leistungsbereitschaft des Schülers als auch zum Umfang des ihm während des Schuljahres vermittelten Wissens. Demgegenüber ist es nicht sachfremd, in Abschlußzeugnissen auf solche Angaben zu verzichten, weil in diesen Fällen die vorstehend genannten Kriterien keine Bedeutung mehr haben.
Die Angaben sind daher nach § 84a Abs. 3 Schulgesetz erforderlich und dürfen auf den Zeugnissen enthalten sein.

2. Es ist zunächst Aufgabe des Schülers selbst, aber auch der Berufsschule, der Erziehungsberechtigten und des Ausbildenden im Betrieb, für eine regelmäßige Teilnahme am Unterricht zu sorgen. Nach den allgemeinen Rechtsgrundsätzen bedeutet dies, daß sich die Berufsschule, wenn sie unentschuldigtes Fehlen im Unterricht feststellt, zunächst an den betroffenen Schüler zu halten hat, sodann an die Erziehungsberechtigten (falls der Schüler noch nicht volljährig ist) und dann an den Ausbilder im Betrieb. Diese Vorgehensweise entspricht nicht nur übergeordneten verfassungsrechtlichen Grundsätzen, sondern trägt auch den in den allgemeinen Gesetzen enthaltenen Forderungen Rechnung, daß der Schüler zunächst selbst in die Pflicht zu nehmen und fürsorglich, aber konsequent zur Leistungsbereitschaft anzuhalten ist. Nur wenn dies ohne Erfolg bleibt, sind weitere Schritte erforderlich.

   Rechtlich zulässig wäre eine andere Vorgehensweise der Schule nur im Ausnahmefall, wenn sich z.B. durch Hinweise des Schülers oder auf anderem Wege tatsächliche Anhaltspunkte ergeben, daß der Ausbilder selbst

oder der Lehrbetrieb den Schüler nicht zum Besuch der Berufsschule freistellen. In diesem Fall würde § 84a Abs. 2 des Schulgesetz i.V.m. § 11 DSG-LSA erlauben, daß die Schule der Handwerksinnung einen Hinweis auf die Pflichtverletzung des Ausbilders bzw. des Lehrbetriebes gibt, weil es auch Aufgabe der Handwerksinnung (und der Handwerkskammer) ist, die Lehrlingsausbildung zu überwachen. Dazu gehört auch, dafür zu sorgen, daß nur solche Betriebe mit der Lehrlingsausbildung beauftragt werden, die die allgemeinen Rechtsvorschriften zum Schulbesuch und die Vorschriften des Berufsausbildungsgesetzes beachten.
Eine namensbezogene Meldung von Fehlzeiten einzelner Schüler in Form von Listen an die Innung ist also im Normalfall weder zulässig noch erforderlich.

3. Es ist ausreichend und rechtlich genügend, wenn die Schule entweder die regelmäßige Unterrichtsteilnahme im Klassenbuch oder in einer Anwesenheitsliste festhält. Zusätzliche Personenkontrollkarten - auch für die Betriebe - sind nicht zulässig.

Die Schule hat zwischenzeitlich von der Führung der Personenkontrollkarte Abstand genommen, vorhandene Exemplare wurden entsprechend § 16 Abs. 2 DSG-LSA vernichtet oder an die Schülerinnen und Schüler ausgehändigt. Auch die übrigen datenschutzrechtlichen Hinweise werden umgesetzt.

Der Landesbeauftragte hat das Kultusministerium gebeten, in geeigneter Weise sicherzustellen, daß die dargestellten datenschutzrechtlichen Anforderungen auch in den anderen Berufsschulen des Landes beachtet werden.

24.3 Anfertigen von Schülerfotos durch private Fotofirmen

Einem Artikel der Mitteldeutschen Zeitung war zu entnehmen, daß in einer Grundschule zum Teil auch gegen den ausdrücklichen Wunsch der Eltern Fotos von Schülern durch eine private Fotofirma gemacht wurden.
Dies hat der Landesbeauftragte zum Anlaß genommen, die datenschutzrechtlichen Aspekte der zuständigen Aufsichtsbehörde aufzuzeigen:

Das Fotografieren von Schülern ohne deren Einwilligung verstößt gegen das in Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG und Art. 6 Abs. 1 der Landesverfassung geschützte Grundrecht auf informationelle Selbstbestimmung der betroffenen Schüler sowie das in Art. 6 Abs. 2 Satz 1 GG und in Art. 11 Abs. 1 Satz 1 der Landesverfassung gewährleistete Elternrecht. Eine Beschränkung dieser Rechte ist nur durch eine gesetzliche Grundlage zulässig, die dem Verfassungsgrundsatz der Verhältnismäßigkeit entspricht und aus der sich die Voraussetzungen und der Umfang der Beschränkungen für die Betroffenen eindeutig und klar ergeben.
Eine solche Rechtsgrundlage fehlt, weil weder das Schulgesetz des Landes Sachsen-Anhalt noch die über § 84a Schulgesetz geltenden allgemeinen Bestimmungen des DSG-LSA das Fotografieren der Schüler ohne deren bzw. die Einwilligung ihrer Sorgeberechtigten gestatten. Bei den betroffenen Grundschülern kann eine rechtswirksame Einwilligungserklärung zum Fotografieren der Kinder nur durch die Personensorgeberechtigten abgegeben werden, weil es diesen Schülern an der nötigen Einsichts- und Entscheidungsfähigkeit fehlt, die vielfältigen Rechtsauswirkungen und insbesondere die besonderen Gefahren eines unachtsamen bzw. mißbräuchlichen Umgangs mit Lichtbildaufnahmen zu übersehen.

Es besteht deshalb eine besondere Pflicht der Schule, vertreten durch den Schulleiter, dafür Sorge zu tragen, daß die Rechte der Kinder gerade in der Schule besonders beachtet werden.

Das vorstehend Ausgeführte gilt entsprechend auch für die Rechte der Eltern. Ihnen obliegt, grundgesetzlich geschützt, in erster Linie die Pflege und Erziehung ihrer Kinder. Eingriffe oder Mißachtungen seitens der staatlichen Schulen in diese Rechte sind nur in gesetzlich genau zugelassenen Fällen erlaubt.
Die Eltern haben dementsprechend gegenüber der Schule einen Anspruch darauf, daß nicht nur die Rechte ihrer Kinder, sondern auch ihre Rechte sorgfältig beachtet werden. Es unterliegt weder der pädagogischen noch der rechtlichen Dispositionsfreiheit eines Schulleiters, seine Entscheidung über das Fotografieren an die Stelle der Elternentscheidung zu setzen. Der Schulleiter kann allenfalls - ggf. nach Rücksprache mit der Schulaufsichtsbehörde - darüber entscheiden, ob Schulzeit für das Fotografieren von Schülern zur Verfügung gestellt werden kann.

Der Landesbeauftragte hat deshalb das Kultusministerium und das in diesem Fall zuständige Regierungspräsidium gebeten, in geeigneter Weise sicherzustellen, daß alle Grundschulen auf die Rechtslage hingewiesen werden.

Ergänzend bat der Landesbeauftragte darum, die dabei für weiterführende Schulen noch verbleibenden Probleme (z.B. Kauf solcher Bilder bei eingeschränkter Geschäftsfähigkeit der Schüler) nicht ungeregelt zu lassen.

Im speziellen Fall wurden die Fotos ordnungsgemäß in der Schule vernichtet. Die Fotofirma wurde von der Schule aufgefordert, die Negative an die Schule zum Zwecke der Vernichtung auszuhändigen.

24.4 Adressen ehemaliger Schülerinnen und Schüler für Klassentreffen

Gelegentlich wenden sich Organisatoren von Klassentreffen ehemaliger Schülerinnen und Schüler mit der Bitte um Adressenübermittlung an ihre alte Schule. Eine Schule hat diese Adressenübermittlung unter Hinweis auf entgegenstehende datenschutzrechtliche Bestimmungen abgelehnt.

Richtig ist, daß eine spezialgesetzliche Regelung für die Datenübermittlung fehlt, weil das Schulgesetz des Landes Sachsen-Anhalt nur auf aktive Schülerinnen und Schüler Anwendung findet. Somit kommt nur das DSG-LSA als gesetzliche Grundlage für die Anschriftenübermittlung in Betracht. Nach § 12 Abs. 1 Ziff. 2 DSG-LSA wäre eine Übermittlung der Daten an den privaten Organisator des Klassentreffens zulässig, wenn er ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und seitens der betroffenen ehemaligen Mitschüler keine schutzwürdigen Interessen entgegenstehen.

Beide Voraussetzungen kann man in solchen Fällen grundsätzlich als gegeben ansehen, wenn der Organisator des jeweiligen Klassentreffens ein ehemaliger Schüler oder ein früher unterrichtender Lehrer ist.

Der Empfänger der Anschriften ist aber darauf hinzuweisen, daß er nach § 12 Abs. 4 DSG-LSA die übermittelten Daten nur für diese Zwecke verarbeiten und nutzen darf (Zweckbindung). Die Nichtbeachtung der Zweckbindung steht nach § 31 Abs. 2 Nr. 2 DSG-LSA unter Strafandrohung.

Eine weitere, alternative Möglichkeit besteht darin, daß der Organisator des Klassentreffens der Schule die entsprechende Anzahl kuvertierter und frankierter Einladungen mit seiner Anschrift als Absender zur Verfügung stellt. Bei dieser Variante versieht die Schule die Umschläge selbst mit Namen und Anschrift der ehemaligen Schüler und versendet sie anschließend. Dann liegt bezüglich dieser Ehemaligen keine Datenübermittlung seitens der Schule vor.

Eine weitere Alternative stellt die Veröffentlichung einer entsprechenden Annonce in der Tagespresse dar.

24.5 Einsichtnahme in Schülerakten

Ein ehemaliger Oberschüler wandte sich an den Landesbeauftragten mit der Bitte, ihm bei der Suche nach der über ihn geführten Schülerakte und der künftig zuständigen Behörde behilflich zu sein. Ferner fragte er an, ob eine Einsichtnahme rechtlich zulässig sei.

Nach Rückfragen beim Kultusministerium konnte ihm folgendes mitgeteilt werden:

Grundsätzlich werden die Schülerakten bei der letzten vom Schüler besuchten Schule aufbewahrt. Bei einer Umstrukturierung ist die Nachfolgerin der Schule für die Aufbewahrung der Schülerakten zuständig. Nachforschungen beim Kultusministerium haben ergeben, daß die Schülerakten nicht vernichtet worden sind, sondern in der Regel aufbewahrt werden.

Auf die weitere Frage, ob eine Einsichtnahme in seine ehemalige Schülerakte rechtlich gedeckt sei, konnte dem Petenten mitgeteilt werden, daß zu den unabdingbaren Rechten des Bürgers jetzt auch das Recht auf Auskunft über die zu seiner Person gespeicherten Daten gehört. Diese Auskunftspflicht nach § 15

Abs. 1 DSG-LSA bezieht sich auch auf die Herkunft oder Empfänger der Daten und den Zweck sowie die Rechtsgrundlage zur Speicherung.

Die speichernde Stelle - also die letzte vom Petenten besuchte Schule - bestimmt das Verfahren, insbesondere die Auskunftserteilung nach pflichtgemäßem Ermessen. Dieser Auskunftspflicht kann nach den Verwaltungsvorschriften zum DSG-LSA auch durch Akteneinsicht Genüge getan werden.

Das Kultusministerium wurde vom Landesbeauftragten gebeten, für eine entsprechende Unterrichtung der Schulen Sorge zu tragen.

24.6 Verarbeitung von Schülerdaten auf privaten Rechnern

Das Kultusministerium ist der Aufforderung des Landesbeauftragten im I. Tätigkeitsbericht (S. 139) nachgekommen und hat einen Erlaß zur Verarbeitung von Schülerdaten auf privaten Rechnern entworfen.

Der Landesbeauftragte wurde im Rahmen der Entwurfserstellung 1993 beteiligt und hat im Februar 1995 die endgültige Entwurfsfassung erhalten. Sie enthält die erforderlichen datenschutzrechtlichen Regelungen. In Kürze ist mit der Veröffentlichung des Erlasses zu rechnen.
Lehrern wird damit die Möglichkeit eröffnet, Schülerdaten unter bestimmten Voraussetzungen auf privaten Rechnern zu verarbeiten.
Da die Lehrkräfte diese Daten aufgrund ihrer besonderen Stellung als Unterrichtende der Schule und damit im Rahmen ihrer Anstellungs- und Beamtenverhältnisse erhalten, bleibt die Schule speichernde Stelle. Als Konsequenz daraus und der Tatsache, daß personenbezogene Daten außerhalb der Schule verarbeitet werden, ist es erforderlich, daß die Lehrkraft spezielle Sicherungsvorkehrungen treffen muß und sich der Kontrolle des Landesbeauftragten unterwirft.

25. Sozialwesen

25.1 Kindertageseinrichtungen

Eine aufmerksame Stadtverwaltung bat beim Landesbeauftragten um Prüfung eines Fragebogens, den das Landesamt für Versorgung und Soziales an die städtischen Kindertageseinrichtungen versandt hatte. Darin wurden umfangreiche personenbezogene Daten der Beschäftigten und der Kinder abgefordert.

Ziel der landesweiten Aktion war es, im Hinblick auf den Rückgang der Kinderzahlen festzustellen, wieviele Einrichtungen mit wievielen Gruppen, Kinder in den Gruppen und wieviele Erzieher derzeit beschäftigt sind, um die Fördermittel des Landes angemessen einsetzen zu können.

Wie die Prüfung ergab, wurde das sicher wichtige Anliegen leider nicht datenschutzgerecht in die Praxis umgesetzt. Die Erhebung und Speicherung personenbezogener Daten bedürfen einer gesetzlichen Grundlage. Die angegebene Rechtsgrundlage (§ 47 SGB VIII) trug die Erhebung von Vor- und Familienname, Geburtsdatum, Zahl der wöchentlichen Arbeitsstunden, Angaben zur Berufsausbildung, Eintrittsdatum in die Einrichtung bei den Beschäftigten und bei allen betreuten Kindern Name und Geburtsdatum nicht.
Die Vorschrift begründet grundsätzlich nur bei der Betriebsaufnahme und der Schließung einer erlaubnispflichtigen Einrichtung sowie der erstmaligen Aufnahme eines Kindes eine Meldepflicht. Der weiteren Begründung, für die Durchführung sowie für die Fortschreibung der Bedarfs- und Entwicklungsplanung seien die Erhebung der personenbezogenen Daten erforderlich, konnte in dieser Komplexität nicht gefolgt werden.
Aus einer vom Gesetz generell übertragenen Aufgabe kann nicht auf die Zulässigkeit einer pauschalen Datensammlung geschlossen werden. Auch die im Gesetz zur Förderung von Kindern in Tageseinrichtungen und die Gewährung von Landeszuwendungen zu den Personalkosten von Kindertageseinrichtungen enthaltenen Vorschriften zur Prüfung der Verwendung von Landesmitteln enthalten keine Rechtsgrundlage für die komplexe Datenerhebung und -speicherung bei

einer Mittelbehörde. Auch die personifizierte Erfassung der Kinder kann allenfalls in der konkreten Einzelfallprüfung, insbesondere der Rechnungsprüfung, von Bedeutung sein, aber nicht pauschal im voraus erfolgen.

Somit fehlt die nach Artikel 6 der Landesverfassung erforderliche gesetzliche Grundlage.

In den Gesprächen mit der obersten Landesbehörde und dem nachgeordneten Landesamt wurde Einigkeit über den Inhalt und die neue Gestaltung der Vordrucke erzielt. Sie entsprechen nunmehr den datenschutzrechtlicher Vorschriften.

Das Recht des Landesamtes für Versorgung und Soziales als Bewilligungsbehörde im Rahmen des § 10 Abs. 3 Satz 1 DSG-LSA Einzelfallprüfungen vorzunehmen, ist durch die getroffene Regelung nicht beeinträchtigt. In diesem Zusammenhang wurde auch angeregt, die kommunalen Rechnungsprüfungsämter in das Prüfverfahren mit einzubeziehen.

25.2 Erhebung personenbezogener Daten bei einem Träger der freien Jugendhilfe

Ein Träger der freien Jugendhilfe wandte sich an den Landesbeauftragten und bat um Aufklärung, ob die Stadt im Rahmen der Beantragung einer Zuwendung berechtigt sei, personenbezogene Daten der Mitarbeiter des Trägers abzufordern. Besonderes Mißtrauen erregte die Abfrage von Lebensläufen und anderen sensitiven Daten.
Darüber hinaus hatte das Jugendamt der Stadt den freien Träger aufgefordert, **alle** abgeschlossenen Arbeitsverträge in Kopie zu übermitteln.
Da der über den Zuschuß entscheidende Jugendhilfeausschuß in öffentlicher Sitzung tagt, wurde auch die Befürchtung geäußert, daß die so vorliegenden personenbezogenen Daten in öffentlicher Sitzung erörtert werden könnten.

Die Stadt berief sich für ihre Vorlageforderungen auf ihre Förderrichtlinien.
Dies reichte nicht aus, denn der Erhebung personenbezogener Daten durch die öffentlichen Stellen sind durch das Grundgesetz und durch die Verfassung des

Landes Sachsen-Anhalt (Art. 6 Abs. 1) enge Grenzen gesetzt. Einschränkungen des Grundrechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse auf **gesetzlicher** Grundlage zulässig. Auch die gesetzlich zugelassenen Eingriffshandlungen müssen dem Gebot der Geeignetheit und Erforderlichkeit entsprechen und den Grundsatz der Verhältnismäßigkeit beachten.
Deshalb hat der Gesetzgeber in § 62 Abs. 1 SGB VII folgerichtig normiert, daß personenbezogene Daten nur erhoben werden dürfen, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgaben erforderlich ist.

An diesen Kriterien waren die Förderrichtlinien der Stadt zu messen. Sie sehen vor, daß die Stadt einen prozentualen Anteil der bei den Trägern der freien Jugendhilfe entstehenden Personalkosten bezuschußt.

Um dazu Vergleichswerte zu erhalten, werden die Tätigkeitsmerkmale und Tätigkeitsbeschreibungen, wie sie der Bundesangestelltentarifvertrag (BAT) vorsieht, analog angewendet. Dazu gehört die Vorlage einer Stellenbeschreibung, die Beifügung von Zeugnissen und **im Einzelfall** ein tabellarischer beruflicher Werdegang, um z.B. bei leitenden Mitarbeitern die Berufspraxis einschätzen zu können.

Aufgrund der Intervention des Landesbeauftragten wird die Stadt zukünftig auf die generelle Vorlage aller Lebensläufe und der Arbeitsverträge verzichten.
In der öffentlichen Sitzung des Jugendhilfeausschusses werden bei den Beschlußvorschlägen nur die Träger als Empfänger und die Zuwendungssummen erörtert. Sofern im Einzelfall eine personenbezogene Diskussion erforderlich wird, ist nach der Geschäftsordnung die Nichtöffentlichkeit des Ausschusses herzustellen.

25.3 Jugendamt und Umgangsrecht mit Kindern

Die Jugendämter haben sich oft mit Problemfällen beim Umgangsrecht geschiedener, getrennt lebender oder nicht verheirateter Eltern mit ihren Kindern auseinanderzusetzen. Zwar trifft das Bürgerliche Gesetzbuch in § 1634 BGB Regelungen für das Umgangsrecht mit ehelichen Kindern und in § 1711 BGB wird grundsätzlich festgestellt, daß der Vater eines nichtehelichen Kindes kein allge-

meines Umgangsrecht hat, doch reichen die beiden dürren Gesetzestexte nicht aus, um die Vielfalt menschlicher Problematik dabei auch nur einigermaßen zu erfassen.

Der Landesbeauftragte hatte es deshalb wiederholt mit Beschwerden von Vätern zu tun (verheirateten wie nicht verheirateten), die das nicht neutrale Verhalten der bei Sorgerechtsentscheidungen oder Besuchsregelungen durch die Gerichte beteiligten Jugendämter bemängelten.
Die Beschwerden waren zum Teil berechtigt, zum Teil unberechtigt. Der Landesbeauftragte nahm deshalb die Fälle zum Anlaß, den Bediensteten strikte Neutralität im Umgang mit den Elternteilen und die ausschließliche Orientierung am Kindeswohl zu empfehlen. Dazu gehört z.B., daß die im Verfahrensrecht vorgeschriebenen Stellungnahmen der Jugendämter stets beiden Elternteilen dann zugänglich sein müssen, wenn sie dem Gericht übermittelt werden.
In keinem Fall zulässig ist es auch, gutachtlich tätige Sachverständige einseitig über Schwächen des einen oder anderen Elternteiles zu informieren, ohne daß dies objektiv nachvollziehbar und aktenkundig ist.

Besonders zu beachten ist die Pflicht zur Amtsverschwiegenheit, womit eine Information von Freunden, Nachbarn oder Verwandten der im Jugendamt zuständigen Bediensteten auch dann nicht zulässig ist, wenn diese zufälligerweise über die Behandlung eines solchen Falles im Jugendamt Kenntnis haben. Der betroffene Bedienstete macht sich u.U. schon strafbar, wenn er auch nur bestätigt, daß ihm der konkrete Fall aus seiner beruflichen Praxis bekannt ist.

25.4 Zahlung von Kindergeld

Wer als Bediensteter bei einer öffentlichen Stelle ungekürztes Kindergeld für das dritte und die folgenden Kinder erhalten will, hat einen Einkommensnachweis zu erbringen. Hierzu sieht das entsprechende bundesweit verwendete Formblatt die Vorlage des Einkommenssteuerbescheides vor. Ein Petent, dem diese Vorlegungspflicht zweifelhaft erschien, hat beim Landesbeauftragten nachgefragt und die folgende Antwort erhalten:

Nach § 60 Abs. 1 Nr. 1 i.V. mit Nr. 3 SGB I hat derjenige, der Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind, sowie Beweismittel zu bezeichnen und auf Verlangen des zuständigen Leistungsträgers Beweisurkunden vorzulegen. Zu den Sozialleistungen zählt auch das Kindergeld (§ 25 Abs. 1 SGB I).

Im Kindergeldverfahren sind Nachweise in der Regel durch Vorlage von Beweisurkunden zu führen. Im Hinblick darauf, daß für das über den Sockelbetrag hinausgehende Kindergeld das Jahreseinkommen des Antragstellers zugrunde gelegt wird (§ 11 Abs. 3 Bundeskindergeldgesetz), bietet sich die Vorlage des Einkommenssteuerbescheides bzw. des Bescheides über die Lohnsteuererstattung als Nachweis an. Legt der Betroffene andere Nachweise vor, ist zu prüfen, ob diese den Beweiszweck ebenfalls erfüllen. Dabei ist zu beachten, daß die genannten Beweispflichten nur insoweit bestehen, als sie zur Feststellung der für die Sozialleistung erheblichen Tatsachen erforderlich sind.
Es ist auch in diesem Verfahren unzulässig, daß die abrechnenden Stellen versuchen, zu Lasten der Betroffenen durch Verwaltungsvorschriften oder Anweisungen (auch Vordrucke gehören dazu) die gesetzlichen Regelungen einzuengen oder fehlende gesetzliche Regelungen zu Einschränkungen zu nutzen.

Es steht also dem Kindergeldberechtigten frei, alle Positionen und Betragsangaben im Einkommenssteuerbescheid, die für die Kindergeldberechnung unbeachtlich sind, durch Schwärzen unkenntlich zu machen. Er kann sein Einkommen auch durch Einzelbescheinigung des Finanzamtes oder vergleichbare Unterlagen nachweisen.
Diese Rechtsauffassung wird inzwischen auch vom Ministerium der Finanzen geteilt.

25.5 Ausgleichsabgabe nach dem Schwerbehindertengesetz

Arbeitgeber der öffentlichen Hand haben, solange sie die vorgeschriebene Anzahl Schwerbehinderter nicht beschäftigen, für jeden unbesetzten Pflichtplatz monatlich eine Ausgleichsabgabe zu entrichten. Diese ist jährlich an die für seinen Sitz zuständige Hauptfürsorgestelle abzuführen. Das Ministerium der

Finanzen nimmt eine Landeszusammenstellung entsprechend der Meldungen der einzelnen Behörden (Personalstellen) vor und weist den Betrag der Ausgleichsabgabe zur Auszahlung an. Da diese Meldungen in den vergangenen Jahren nicht termingerecht vorlagen, fragte das Ministerium der Finanzen (MF) beim Landesbeauftragten an, ob nicht vorsorglich die Speicherung der Schwerbehinderung sowie des Grades der Schwerbehinderung im Bezüge-ADV-Verfahren möglich wäre.

Der Landesbeauftragte hält ein solches Vorhaben für gesetzlich nicht zulässig.

Ausgangspunkt für die datenschutzrechtliche Prüfung ist § 35 Abs. 1 Satz 1 SGB I. Danach hat jeder Anspruch darauf, daß Einzelangaben über seine persönlichen und sachlichen Verhältnisse (personenbezogene Daten) von den Leistungsträgern als Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden. Das Datum der Schwerbehinderung sowie der Grad der Behinderung sind jeweils für sich personenbezogene Daten und unterliegen dem Sozialgeheimnis. Eine Übermittlung dieser Daten an Dritte wäre deshalb nur in den gesetzlich vorgesehenen Ausnahmefällen zulässig.
Die vom MF vorgesehene Übermittlung personenbezogener Sozialdaten von den jeweils zuständigen Personaldienststellen an die Bezügestellen und die dort vorgesehene Speicherung des Datums Schwerbehinderter und Grad der Behinderung sind in § 13 Abs. 2 SchwbG nicht vorgesehen. Der Schwerbehinderte muß es deshalb nicht hinnehmen, bei einer dritten Stelle (hier: Bezügestelle) bekannt und gespeichert zu werden; es sei denn, er willigt in die Übermittlung seiner Daten ein (§ 67 Nr. 1 SGB X).

25.6 Jugendhilfe

Schwierig gestaltete sich die Einarbeitung datenschutzrechtlicher Grundregelungen in die vom Ministerium für Arbeit, Soziales und Gesundheit erstellten Richtlinien für Hilfen zur Erziehung, Eingliederungshilfen für Behinderte und Jugendliche, Hilfen für junge Volljährige und den Schutz von Kindern und Jugendlichen in Familienpflege und Einrichtungen.

Im Entwurf fehlten die erforderlichen Hinweise auf den im 4. Kapitel des SGB VIII enthaltenen bereichsspezifischen Datenschutz und auch andere wichtige Regelungen für eine datenschutzfreundliche Anwendung. Erst nach massiven Gegenvorstellungen gelang es mit Unterstützung des Ministeriums des Innern, das Fachministerium zur Überarbeitungen des Erlaßentwurfs in den Punkten zu bewegen, die die Rechte der Betroffenen einschränkten.

Inwieweit diese Richtlinien wegen der häufigen Verweisungen auf andere Rechtsvorschriften anwenderfreundlich sind, muß abgewartet werden.

26. Stasi-Unterlagen-Gesetz

In seinem I. Tätigkeitsbericht (S. 144 ff) hatte der Landesbeauftragte bereits über das Inkrafttreten des Stasi-Unterlagen-Gesetzes (StUG) informiert und von seiner Kritik an der beabsichtigten, seiner Meinung nach aber unzureichenden, Änderung der §§ 18 und 24 StUG berichtet. Die Änderungen seitens des Bundesgesetzgebers stehen bis heute aus.

Von der in § 38 StUG vorgesehenen Möglichkeit, durch Landesgesetz die Institution eines Landesbeauftragten zur Wahrnehmung der Bürger- und Landesinteressen nach dem Stasi-Unterlagen-Gesetz zu schaffen, wurde mit dem Ausführungsgesetz zum Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (AG StUG LSA) vom 18.08.1993 Gebrauch gemacht. Der Landesbeauftragte war an dem Gesetzgebungsvorhaben beteiligt und seine Anregungen haben Eingang in den Gesetzestext gefunden.

Der Landesbeauftragte nimmt die zwischenzeitlich gemachten Erfahrungen bei Prüfungen im Lande zum Anlaß, noch einmal ausdrücklich auf die gesetzliche Verpflichtung (§§ 7 ff StUG) aller öffentlichen Stellen, natürlichen Personen und sonstigen nichtöffentlichen Stellen des Landes hinzuweisen, den Besitz von Unterlagen des Staatssicherheitsdienstes beim Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR in Berlin anzuzeigen und diese Unterlagen auf Verlangen herauszugeben.

27. Statistik

27.1 Fehlendes Landesstatistikgesetz

Bereits 1992 wurde deutlich, daß in Sachsen-Anhalt ein Landesstatistikgesetz fehlt. Das Ministerium des Innern legte auch Anfang 1993 einen Arbeitsentwurf zur Stellungnahme vor. Die vom Landesbeauftragten dazu eingebrachten Vorschläge und Anregungen fanden im wesentlichen Berücksichtigung. Doch im folgenden Verfahren geriet der Entwurf in die allgemeinen politischen Wirren des Landes. Erst im Dezember 1994 wurde nun auch auf Drängen des Landesbeauftragten durch die Landesregierung ein Gesetzentwurf beschlossen und in das parlamentarische Gesetzgebungsverfahren eingebracht.
Der Landesbeauftragte appelliert nun an den Landtag, den Gesetzentwurf im Hinblick auf die berechtigten Erwartungen der Bürger und der betroffenen öffentlichen Stellen zügig zu beraten.

27.2 Statistische Daten und ihre Geheimhaltung

Das Statistische Landesamt Sachsen-Anhalt sieht eine seiner Hauptaufgaben in der Veröffentlichung statistischer Ergebnisse und der möglichst weiten Abdeckung des immer größer werdenden Informationsbedarfes. Dabei setzt ihm jedoch das Statistikgeheimnis Grenzen.
So schreibt § 16 Abs. 1 BStatG vor, daß Einzelangaben über persönliche oder sachliche Verhältnisse, die für eine Bundesstatistik gemacht werden, geheimzuhalten sind, soweit durch Rechtsvorschriften nichts anderes bestimmt ist. Das gilt jedoch u.a. nicht für Einzelangaben, die von einem Statistischen Amt mit den Einzelangaben anderer Befragter zusammengefaßt und in statistischen Ergebnissen dargestellt werden und auch nicht für solche Einzelangaben, die einem Befragten oder Betroffenen nicht zugeordnet werden können.

Dabei kommt es in der täglichen Praxis immer wieder zu Zweifelsfällen. So fragte das Statistische Landesamt beim Landesbeauftragten an, ob gegen Tabellen statistischer Ergebnisse mit Feldern, in denen das Erhebungsmerkmal nur in ein oder zwei Fällen auftritt, datenschutzrechtliche Bedenken erhoben werden können.

Der Landesbeauftragte verwies darauf, daß im Einzelfall zu prüfen sei, ob solche Einzelangaben im Ergebnis dazu führen können, daß die betroffene natürliche Person bestimmbar wird. Dann ist das Statistikgeheimnis nicht mehr gewahrt. Dabei spielt die Gesamtsumme der Befragten bzw. der Einzelfälle ebenso eine Rolle wie die territoriale Aufschlüsselung und/oder die Untergliederung der Fälle in mehr oder weniger breite Altersstufen.
In den mit der Anfrage des Statistischen Landesamtes vorgelegten Tabellenbeispielen war **ein** Fall von Malaria eines Mädchens im Alter von 5 bis 15 Jahren für ganz Sachsen-Anhalt genannt. Diese statistische Angabe war unproblematisch. Anders wäre dies zu beurteilen gewesen, wenn sich der Fall auf eine Gemeinde mit wenigen hundert Einwohnern bezogen hätte.

Der Landesbeauftragte gab die Empfehlung, Zusammenstellungen statistischer Ergebnisse, die einzelne Fälle enthalten (also Tabelleneinsen oder auch -zweien), stets auf die Möglichkeit der Deanonymisierung hin zu untersuchen.
In Zweifelsfällen sollte bei Gefahr der Deanonymisierung das geltende Gebot der Dreier-Aggregation beachtet werden.

27.3 Novellierung des Mikrozensusgesetzes

Auf Bundesebene wird die Änderung und Ergänzung des Mikrozensusgesetzes vorbereitet. Einen ersten Arbeitsentwurf hat das Bundesministerium des Innern jetzt vorgelegt. Dieses Gesetz hat auch für die Bürger Sachsen-Anhalts erhebliche Bedeutung, denn es verlangt vom zufällig ausgewählten Bürger die Beantwortung vieler detaillierter Fragen zur wirtschaftlichen und sozialen Lage der Familie, zum Arbeitsverhältnis, zur beruflichen Ausbildung und zu seinen Wohnverhältnissen.
Der Landesbeauftragte mußte nach einer ersten Prüfung feststellen, daß der neue Gesetzentwurf aus datenschutzrechtlicher Sicht hinter dem zur Zeit geltenden Schutzstandard mit überschaubaren Fragekomplexen und dem Recht zur freiwilligen Antwort in Teilbereichen weit zurück bleibt.
Ziel der Novellierung ist die Aufnahme dutzender neuer Erhebungsmerkmale, die Verkürzung der Periodizität und die Erhöhung des Auswahlsatzes der Befragten, vor allem aber eine erhebliche Ausweitung der Auskunftspflicht.

Nach Ansicht des Landesbeauftragten läßt dieser Entwurf jedes Maß an Ausgewogenheit vermissen, wie es das Bundesverfassungsgericht im bekannten Volkszählungsurteil dem Gesetzgeber auferlegt hat, wenn er das Grundrecht der Bürger auf informationelle Selbstbestimmung einschränken will.

Dementsprechend wäre konsequenterweise zu fordern, daß nur diejenigen Angaben zwangsweise erhoben werden dürfen, bei denen der Zweck der Statistik mit freiwilligen Auskünften nicht erreicht werden kann.
Auch die im vorliegenden Gesetzentwurf vorgesehene Verkürzung der Periodizität und die Vergrößerung des Auswahlsatzes würde die verfassungsrechtlich garantierte Freiheit des Bürgers einschränken und bedarf einer eingehenden, auch wissenschaftlich unterlegten Begründung zur Erforderlichkeit.

Das Ministerium des Innern wurde deshalb vom Landesbeauftragten gebeten, sich bei den anstehenden Fachberatungen dafür einzusetzen, daß die schon einmal 1990 durch den Bundesrat vorgebrachten Wünsche auf Ausweitung des Mikrozensus kritisch überdacht werden.

27.4 Mikrozensuserhebung

In seinem I. Tätigkeitsbericht (S. 147) mußte der Landesbeauftragte über Probleme des Statistischen Landesamtes bezüglich dessen Umgang mit den Bürgern bei der Vorbereitung und Durchführung des Mikrozensus berichten, auf die ihn viele Bürgerinnen und Bürger aufmerksam gemacht hatten.
Auch in diesem Berichtszeitraum war der Mikrozensus Anlaß für viele betroffene Bürgerinnen und Bürger, sich mit Fragen oder der Bitte um Erläuterungen an den Landesbeauftragten zu wenden. In der Regel drehten sich die Anfragen um die Rechtmäßigkeit der Befragungen, Fragen zur Auskunftspflicht und der Folgen der Auskunftsverweigerung.
Begründete Beschwerden gab es jedoch keine mehr.

27.5 Verknüpfung verschiedener Statistiken

Das Bundesministerium für Wirtschaft beabsichtigte 1993, zur Gewähr einer aussagefähigen Erfolgskontrolle der Gemeinschaftsaufgabe „Verbesserung der regionalen Wirtschaftsstruktur“, die Entwicklung der geförderten Betriebe mit der Entwicklung der nicht geförderten zu vergleichen.
Gegen dieses Vorhaben ist, vor allem vor dem Hintergrund des möglichst wirtschaftlichen Einsatzes der verfügbaren Haushaltmittel, nichts einzuwenden.
Allerdings war beabsichtigt, dies durch Verknüpfung von Daten der in eine Förderbetriebsstatistik überführte Förderfallstatistik der Gemeinschaftsaufgabe mit Daten aus der (Bundes-) Statistik im Produzierenden Gewerbe zu tun.
Das Statistische Bundesamt hatte gegen das Vorhaben erhebliche rechtliche Bedenken.
Vom Ministerium für Wirtschaft und Technologie (MW) wurde der Landesbeauftragte um Überprüfung gebeten, ob er die Bedenken des Statistischen Bundesamtes teilt.

Der Landesbeauftragte hat sich der Auffassung des Statistischen Bundesamtes angeschlossen. Die datenschutzrechtliche Bewertung der Zulässigkeit einer solchen Verknüpfung ist nur anhand der bereichsspezifischen Regelungen im BStatG bzw. dem ProdGewStatG möglich. Dort fehlt die erforderliche Rechtsgrundlage. Statt dessen wird in beiden Gesetzen der Wille des Gesetzgebers deutlich, der Übermittlung bzw. Nutzung von Einzelangaben - auch und gerade durch das Zusammenführen von Daten aus mehreren Statistiken - enge Grenzen zu setzen. Ein Beispiel enthält § 13a Abs. 1 BStatG, der die Nutzung von Datensätzen aus Bundesstatistiken für Zusammenführungen auf die nach dieser Regelung ermöglichten Fälle beschränkt.

Der Landesbeauftragte konnte dem MW deshalb nur mitteilen, daß allenfalls die Möglichkeit besteht, die Betriebsnummer der amtlichen Statistik im produzierenden Gewerbe im Fördermittelantragsformular auf **freiwilliger** Basis mit entsprechendem deutlichem Hinweis zu erheben, um die Erfolgskontrolle der Regionalförderung wenigsten teilweise zu gewährleisten.

27.6 Vorbereitung der Gebäude- und Wohnungszählung 1995

Nach dem WoStatG findet zum Stichtag 30.09.1995 in den neuen Bundesländern die Gebäude- und Wohnungszählung statt.
Dabei kommt auf die Gemeinden/Verwaltungsgemeinschaften eine Fülle von Aufgaben zu, bei deren Lösung auch datenschutzrechtliche Gesichtspunkte beachtet werden müssen.

Den für die Zählungsvorbereitung Verantwortlichen hat der Landesbeauftragte auf Anfragen folgende Hinweise gegeben:

a) § 3 Abs. 1 der Verordnung zur Durchführung des WoStatG legt fest, daß die durch die Gemeinden bzw. Verwaltungsgemeinschaften zu bildenden Erhebungsstellen nicht nur räumlich, sondern auch organisatorisch und personell von anderen Verwaltungsstellen zu trennen sind.

b) Wegen der Fülle der dann in den Erhebungsstellen vorhandenen personenbezogenen Daten sind technische und organisatorische Maßnahmen zum Schutz der Daten nach § 6 Abs. 2 DSG-LSA besonders sorgfältig zu planen und umzusetzen. Hierzu sind durch den Landesbeauftragten Prüfungen und Kontrollen beabsichtigt.

c) Bei der Aufstellung des Verzeichnisses der Straßen- und Hausnummern und der Ermittlung der Eigentümer werden auch Übermittlungen personenbezogener Daten von anderen öffentlichen Stellen an die Erhebungsstellen erforderlich. Die Ämter und Stellen, die zur Übermittlung berechtigt bzw. verpflichtet sind, sind in § 8 Abs. 1 bis Abs. 3 WoStatG abschließend aufgezählt. Nur wenn bei bestimmten Gebäuden jeder Personenbezug fehlt, kann auf Angaben von anderen Ämtern (Entsorgung, Umwelt, Wirtschaft) zurückgegriffen werden.

d) Im übrigen ist auch bei den Erhebungsstellen darauf zu achten, daß eine Meldung zum Dateienregister zu erstatten ist, wenn nicht der Ausnahmefall des § 14 Abs. 3 DSG-LSA zutrifft.

27.7 Sozialhilfestatistik

Dem Landesbeauftragten war bekannt geworden, daß in anderen Bundesländern seit dem 01.01.1994 im Rahmen der Sozialhilfestatistik personenbezogene Daten erhoben werden, für die es im BSHG keine Rechtsgrundlage gibt und die nur für die Statistik, nicht jedoch für die Leistungsgewährung erforderlich sind.
Das Ministerium für Arbeit, Soziales und Gesundheit (MS) ist diesbezüglich durch den Landesbeauftragten darauf hingewiesen worden, daß es sich bei der Sozialhilfestatistik um eine sogenannte Sekundärstatistik handelt. Für diese dürfen nur solche Daten genutzt werden, die im Rahmen des Verwaltungsvollzuges, also im jeweiligen Einzelfall bei der Gewährung von Sozialhilfe angefallen und erhoben worden sind. Auskunftspflichtig ist allein der Sozialhilfeträger. Eine Datenerhebung beim Betroffenen, etwa mittels Fragebogen, ist - in diesem Fall auch auf freiwilliger Basis - unzulässig. Dafür wäre eine besondere gesetzliche Grundlage erforderlich.
Vorsorglich wurde darauf hingewiesen, daß bereits unzulässigerweise für die Sozialhilfestatistik zusätzlich erhobene personenbezogene Daten im Wege der Folgenbeseitigung ungenutzt zu löschen sind.
Eine Antwort des MS steht zur Zeit noch aus.

28. Strafvollzug

28.1 Datenschutz im Strafvollzug

Im Sommer 1994 hat die im I. Tätigkeitsbericht (S. 150) bereits erwähnte Informationsveranstaltung zum Thema "Datenschutz im Strafvollzug" mit den Anstalts- und Abteilungsleitern stattgefunden.
Der Landesbeauftragte wies dabei auf die datenschutzrechtlichen Grundlagen unter Berücksichtigung der besonderen Aspekte des Strafvollzuges hin und machte deutlich, daß gerade dort das individuelle Recht auf informationelle Selbstbestimmung in besonderer Weise berührt wird. Eingriffe in dieses Recht bedürfen nach Art. 6 Abs. 1 der Landesverfassung einer bereichsspezifischen,

normenklaren Rechtsgrundlage, die im Strafvollzugsgesetz nicht immer zu finden ist. Dabei hat der Strafgefangene grundsätzlich die gleichen Rechte wie ein freier Bürger.
Es fehlen aber auch gesetzliche Regelungen über die Verarbeitung personenbezogener Daten dritter Personen, die mit einem Strafgefangenen in Verbindung stehen (z.B. Verwandte, Lebenspartner, Geschäftspartner).

Ein vom Bundesministerium der Justiz (BMJ) erstmals 1991 vorgelegter vorläufiger Referentenentwurf zur Änderung des Strafvollzugsgesetzes ist seinerzeit von den Datenschutzbeauftragten des Bundes und der Länder kritisch gewürdigt worden. Ein überarbeiteter Entwurf fehlt bis heute.
Mangels bereichsspezifischer Rechtsgrundlagen hat sich deshalb die Datenverarbeitung und Nutzung in den Vollzugsanstalten auf das absolut notwendige Minimum zu beschränken. Übergangsweise gilt ergänzend das DSG-LSA (vgl. § 3 Abs. 3 DSG-LSA).

Der Landesbeauftragte wird im kommenden Berichtszeitraum auch in Vollzugsanstalten gem. § 22 Abs. 1 DSG-LSA datenschutzrechtliche Kontrollen durchführen.

28.2 Zugriff auf Gefangenenpersonalakten

Von einem Kollegen wurde dem Landesbeauftragten mitgeteilt, daß er anläßlich der datenschutzrechtlichen Kontrolle einer Justizvollzugsanstalt festgestellt habe, daß alle Vollzugsbediensteten jederzeit Zugriff auf alle vollständigen Gefangenenpersonalakten haben.

Eine derartig weitgefaßte Zugriffsbefugnis hält auch der Landesbeauftragte für sehr bedenklich. Eine Einsicht in die Gefangenenpersonalakte kann nach der Rechtslage nur in dem Umfang erfolgen, der zur jeweiligen Aufgabenerfüllung erforderlich ist. Mithin können grundsätzlich nur die Bediensteten Zugriff auf die Gefangenenpersonalakte erhalten, die den Gefangenen unmittelbar betreuen oder für die die Kenntnis der Gefangenenpersonalakte aus sonstigen Gründen zur Erfüllung dienstlicher Aufgaben im Einzelfall erforderlich ist.

Der Landesbeauftragte nahm dies deshalb zum Anlaß, das Ministerium der Justiz (MJ) zur Arbeitsweise in Sachsen-Anhalt zu befragen. Nach der Antwort des Ministeriums ist die Praxis in den Justizvollzugsanstalten des Landes datenschutzgerechter.
Zugriff auf alle Akten haben lediglich der Anstaltsleiter und der Vollzugsleiter, und auf die Akten der jeweiligen Abteilung der zuständige Vollzugsabteilungsleiter und der Sicherheitsdienstleiter. Dem sozialen Dienst und dem Anstaltspsychologen wird über den Vollzugsabteilungsleiter im Einzelfall die Gefangenenpersonalakte zugeleitet, wenn sie zu Stellungnahmen (z.B. zur Gewährung von Vollzugslockerungen, zur vorzeitigen Entlassung usw.) aufgefordert werden. Alle übrigen Bediensteten haben auf die Gefangenenpersonalakten keinen unmittelbaren Zugriff. Ihnen werden nur Teile der Gefangenenpersonalakte eines bestimmten Gefangenen zugeleitet, wenn sie über einen Sachverhalt (z.B. besondere Fluchtgefahr, Suizidgefahr) unterrichtet werden müssen. Die Krankenakten der Gefangenen, die Teil der Gefangenenpersonalakte sind, werden nicht in den Vollzugsgeschäftsstellen, sondern beim Anstaltsarzt aufbewahrt. Auf diese Aktenteile haben lediglich der Anstaltsarzt und das Krankenabteilungspersonal Zugriff.

Mit dieser Verfahrensweise wird nach Auffassung des Landesbeauftragten in den Vollzugsanstalten in Sachsen-Anhalt den datenschutzrechtlichen Belangen in ausreichender Weise Rechnung getragen.
Der Landesbeauftragte wird die Praxis im Rahmen seiner Prüftätigkeit näher beleuchten.

29. Umwelt und Natur

29.1 Einsichtsrecht in Umweltakten

Mit Gesetz vom 08.07.1994 (BGBl. I S. 1490) hat der Bundestag das Umweltinformationsgesetz (UIG) verabschiedet und damit die entsprechende EG-Richtlinie vom 07.06.1990 über den freien Zugang zu Informationen über die Umwelt umgesetzt. Jetzt hat jedermann Anspruch auf freien Zugang zu behördlichen Umweltinformationen. Allerdings bleibt es der zuständigen Behörde

überlassen, ob sie das Informationsbegehren durch Gewährung von Akteneinsicht, durch Auskunftserteilung oder auf sonstige Weise erfüllt.

Der Informationsanspruch gilt jedoch nicht einschränkungslos und wird zum Schutz öffentlicher Belange (§ 7 UIG) bzw. zum Schutz privater Belange (§ 8 UIG) unter den dort im einzelnen genannten Voraussetzungen ausgeschlossen. Insbesondere ist zur Wahrung des Rechts auf informationelle Selbstbestimmung das Einsichtsrecht ausgeschlossen, soweit in Folge der Offenbarung personenbezogener Daten schutzwürdige Interessen der Betroffenen beeinträchtigt würden oder der Schutz geistigen Eigentums - insbesondere Urheberrechte - der Auskunftserteilung oder der zur Verfügungstellung von Informationsträgern entgegenstehen. Auch Betriebs- und Geschäftsgeheimnisse dürfen nicht unbefugt offenbart werden. Ferner besteht der Anspruch dann nicht, wenn die gewünschten Informationen dem Steuergeheimnis oder dem Statistikgeheimnis unterliegen.

Vor allem diese materiellen Ausschluß- und Beschränkungsgründe sind wenig "gerichtsfest" formuliert und dürften zu Anwendungsschwierigkeiten in der Praxis führen und Anlaß zu Rechtsstreitigkeiten geben.

Das Institut für Weiterbildung und Beratung im Umweltschutz e.V. hat in einem Tagesseminar interessierten Bürgern Informationen zu diesem Thema angeboten. Der Landesbeauftragte hat sich mit einem eigenen Beitrag an der Veranstaltung beteiligt.

29.2 Sonderabfallbeseitigung

Eine obere Landesbehörde wandte sich an den Landesbeauftragten mit der Frage, ob Daten aus den Betriebskatastern der Gewerbeaufsichtsverwaltung an eine Beratungsgesellschaft übermittelt werden dürfen.
Hintergrund war, daß ein Ministerium eine Beratungsgesellschaft beauftragt hatte, Recherchen für ein Sonderabfallwirtschaftskonzept durchzuführen. In diesem Zusammenhang wandte sich die Beratungsgesellschaft an verschiedene Aufsichtsbehörden, um die Anzahl der betroffenen Betriebe sowie die Anzahl der in diesen Betrieben Beschäftigten zu ermitteln.

Der Landesbeauftragte sah in der Übermittlung dieser Daten kein datenschutzrechtliches Problem, da es sich bei der numerischen Angabe der Beschäftigten in Einrichtungen nicht um personenbezogene Daten handelt. Um personenbezogene Daten würde es sich handeln, wenn Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (Betroffene) erhoben und übermittelt würden. Dieses war hier nicht der Fall.

30. Verfassungsschutz

30.1 NADIS-Richtlinien

Das Bundesamt für Verfassungsschutz und die Verfassungsschutzämter der Länder führen gemeinsam auf bundesgesetzlicher Grundlage ein Nachrichtendienstliches Informationssystem (NADIS). Dazu hat der Bund neue Richtlinien für die Verarbeitung und Nutzung personen- und sachbezogener Daten erarbeitet. Die Richtlinien sind von der Innenministerkonferenz des Bundes und der Länder im Mai 1994 zustimmend zur Kenntnis genommen worden.

Der Landesbeauftragte hatte zuvor gegenüber dem Ministerium des Innern zum Entwurf dieser Richtlinien Stellung genommen und datenschutzrechtliche Verbesserungen und Klarstellungen angeregt. Es erging ihm aber nicht besser als seinen Kollegen in den anderen Ländern auch. Die vom Bund dominierten Verhandlungen führten nicht dazu, daß diese Anregungen und Hinweise Eingang in die Richtlinien gefunden hätten.

Insbesondere zwei Bestimmungen in der Richtlinie sind wegen ihrer direkten negativen Auswirkung auf Betroffene besonders bedenklich:

30.1.1 Ek-Datum

Das in § 8 Abs. 5 angesprochene Ek-Datum (Stand der letzten Erkenntnis/ Information) hat große Bedeutung für die spätere Löschung, ist aber inhaltlich hinsichtlich seiner Bedeutung nicht ausreichend bestimmt. Da die EDV bei jeder

Neu-/Veränderungseingabe automatisch ein neues Ek-Datum speichert, kann schon eine geänderte Anschrift die generelle 5-Jahres-Prüffrist für Löschungen neu begründen. Eine solche Verfahrensweise ist materiell-rechtlich nicht gedeckt.
Der Landesbeauftragte hatte deshalb übereinstimmend mit dem Bundesbeauftragten und anderen Landesbeauftragten angeregt, in den Richtlinien den Begriff des "Ek-Datums" näher zu definieren. Das hat das BMI abgelehnt mit dem Hinweis, in den Arbeitsplänen des **BfV** sei der Begriff des Ek-Datums ausreichend geregelt.
Der Verweis auf diese Arbeitspläne reicht nach Auffassung des Landesbeauftragten bei einem Verbundsystem des Bundes **und der Länder** nicht aus. Es sollte auch aus der Sicht der Verfassungsschutzbehörden ein Interesse daran bestehen, eine einheitliche Praxis bei der Vergabe dieses Datums zu gewährleisten.

Dem Landesbeauftragten ist in einem Gespräch mit dem Landesamt für Verfassungsschutz für die Bearbeitungsfälle des Landes zugesagt worden, daß das Ek-Datum für sich gesehen kein Kriterium für die Prüffrist zur Löschung sein soll, sondern diese mit einer gesondert festzusetzenden Wiedervorlagefrist gewährleistet wird.

30.1.2 Protokollierungspflicht

§ 9 Abs. 1 der Richtlinien enthält eine generelle Protokollierungspflicht u.a. **aller** Speicherungen, Löschungen und Einsichtnahmen. Eine zur Kontrolle grundsätzlich wünschenswerte Protokollierung darf aber nicht dazu führen, daß damit ein neuer Informationsfundus geschaffen wird, auf den unbeschränkt zurückgegriffen werden kann. In vergleichbaren Fällen wird daher der Zufallsprotokollierung der Vorzug eingeräumt, bei der z.B. ca. jede 20., 50. oder 100. Datenbewegung aufgezeichnet wird.
In diesem Punkt bestehen keine Abhilfemöglichkeiten beim Landesamt für Verfassungsschutz.

30.2 Sicherheitsüberprüfung

Der Landesbeauftragte hat im Berichtszeitraum auch die Einhaltung datenschutzrechtlicher Bestimmungen bei der Durchführung der Sicherheitsüberprüfungen durch das Landesamt für Verfassungsschutz (LfV) geprüft.

Das LfV führt die Sicherheitsüberprüfungen nicht von sich aus durch, sondern wirkt nach § 4 Abs. 2 Nr. 1 und 2 VerfSchG-LSA auf Ersuchen des zuständigen Geheimschutzbeauftragten der jeweiligen Dienststelle des Betroffenen bei der Sicherheitsüberprüfung mit.
Dazu bedarf es der Einwilligung der betroffenen Person; das gilt auch, wenn eine erweiterte Überprüfung beantragt ist, für die Einbeziehung des Ehegatten, Verlobten oder der Person, die mit dem Betroffenen in einer Lebensgemeinschaft zusammenlebt. Das Landesamt darf dabei die im Rahmen der Überprüfung erforderlichen Informationen, einschließlich personenbezogener Daten, erheben, verarbeiten und nutzen. Um den in § 6 VerfSchG-LSA verankerten Grundsatz der Verhältnismäßigkeit auch im Rahmen der Sicherheitsüberprüfungen zu gewährleisten, sind abgestufte Überprüfungstiefen (Ü1 bis Ü3) vorgesehen. Die Einzelheiten des Verfahrens sind in den Richtlinien für die Sicherheitsüberprüfung von Personen im Rahmen des Geheimschutzes (SiR-LSA) vom 19.10.1992 (MBl. LSA S. 1822) geregelt. Bei deren Erstellung sind eine Vielzahl von Hinweisen und Anregungen des Landesbeauftragten eingeflossen.

Insgesamt bewertet hat die Prüfung beim Landesamt keine schwerwiegenden datenschutzrechtlichen Mängel ergeben. Die vorstehend dargelegten Rechtsgrundlagen und Verfahrenswege wurden beachtet. Fehleinstufungen beim Grad der Sicherheitsüberprüfung wurden nicht festgestellt. Die zu überprüfenden Bediensteten wurden nach Aktenlage unterschiedslos gleich behandelt (keine West-Ost-Differenzierung).

Das befriedigende Ergebnis der Prüfung geht auch auf zwei vom LfV in den Jahren 1993 und 1994 selbst vorgenommene Überprüfungen und Überarbeitungen der in den Akten gespeicherten personenbezogenen Daten zurück, bei denen auch zuviel erhobene Daten gelöscht wurden.

30.3 Mitwirkung der Verfassungsschutzbehörden im Einbürgerungsverfahren

Eine Anfrage des Bundesbeauftragten für den Datenschutz nahm der Landesbeauftragte zum Anlaß, die Praxis der Mitwirkung der Verfassungsschutzbehörden bei Einbürgerungen zu untersuchen.

Nach den einschlägigen Vorschriften (z.B. §§ 8 f RuStAG, §§ 6 ff 1.StARegG, §§ 85, 86 AuslG) setzt eine Einbürgerung u.a. voraus, daß der Ausländer die innere oder äußere Sicherheit der Bundesrepublik Deutschland nicht gefährdet. In Sachsen-Anhalt wird diese Bestimmung nach Mitteilung des Ministeriums des Innern dahingehend ausgelegt, daß die zuständigen Behörden bei tatsächlichen Anhaltspunkten für eine politisch extremistische Betätigung des Einbürgerungsbewerbers eine Anfrage an das Landesamt für Verfassungsschutz richten. Eine sogenannte Regelanfrage erfolgt nicht.

Gemäß § 18 Abs. 1 VerfSchG-LSA darf die Verfassungsschutzbehörde personenbezogene Daten an inländische Behörden übermitteln, wenn der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt.

Der Landesbeauftragte hält die für Sachsen-Anhalt mitgeteilte Verwaltungspraxis für datenschutzgerecht. Er hat gegenüber dem Ministerium des Innern angekündigt, deren Einhaltung im Rahmen seiner Prüftätigkeit zu kontrollieren.

31. Verkehr

31.1 Automatische Gebührenerhebung (AGE) auf Autobahnen in Deutschland

Erstmals im April 1993 fanden Gespräche zwischen dem Bundesministerium für Verkehr als Auftraggeber für den Feldversuch auf der Bundesautobahn A 555 (Streckenabschnitt Bonn/Nord - Wesseling), den mit der Durchführung des

Feldversuches beauftragten Unternehmen und Vertretern des Bundesbeauftragten für den Datenschutz (BfD) statt. 1994 haben auch die Datenschutzbeauftragten der Länder Gelegenheit gehabt, sich vor Ort ein Bild der technischen Anwendungsmöglichkeiten zu verschaffen.
Kernpunkt der seit dieser Zeit stattfindenden Gespräche und Überlegungen ist die datenschutzrechtliche Forderung, auch künftig auf allen in Frage kommenden Verkehrswegen (Autobahnen oder Stadtstraßen) eine "datenfreie Fahrt" zu gewährleisten, d.h. über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürften keine Daten erhoben oder verarbeitet werden. Ansonsten wären für den einzelnen nicht mehr kontrollierbare und wegen ihrer vielfältigen Verwendbarkeit gefährliche Bewegungsprofile die Folge.

Aus datenschutzrechtlicher Sicht bieten AGE-Systeme, die auf der Vorausbezahlung der Gebühren basieren (**Prepaid-Verfahren**), bessere Voraussetzungen zur Wahrung der Anonymität als Systeme, bei denen nach einer Datenerhebung und -speicherung diese dann dem Benutzer in Rechnung gestellt bzw. von seinem Konto abgebucht werden (**Postpaid-Verfahren**).
Je weniger personenbezogene oder personenbeziehbare Daten bei einer automatischen Gebührenerhebung erfaßt, verarbeitet oder genutzt werden, desto geringer ist auch die Möglichkeit einer mißbräuchlichen Datennutzung.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb auf ihrer 49. Konferenz am 09./10.03.1995 dazu eine Entschließung gefaßt, die die wesentlichen Forderungen zur Gewährleistung eines für alle Bürger ausreichenden Datenschutzes enthält **(Anlage 17).**

Nach dem Abschluß des Feldversuches im Sommer diesen Jahres ist noch 1995 eine Grundsatzentscheidung des Bundesministeriums für Verkehr zu diesem Thema zu erwarten.

31.2 Verwertung strafrechtlicher Verurteilungen bei der Erteilung oder Entziehung der Fahrerlaubnis

Grundsätzlich darf eine getilgte Eintragung über die Tat und die strafrechtliche Verurteilung dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten und nicht mehr zu seinem Nachteil verwertet werden.
Nach § 52 Abs. 2 BZRG gilt dieses Verwertungsverbot aber nicht in Verfahren zur Erteilung oder Entziehung einer Fahrerlaubnis. Vom Verwertungsverbot sind danach alle strafrechtlichen Verurteilungen ausgenommen, die in das Verkehrszentralregister (VZR) eingetragen wurden, auch wenn sie dort nach den vorgegebenen Tilgungsfristen schon gelöscht sind.
In der Verwaltungspraxis der Straßenverkehrsbehörden finden sich deshalb, wie aus Kontrollen der Landesbeauftragten in den alten Bundesländern bekannt ist, zum Teil bis zu 30 Jahre alte Entscheidungen in den Akten.

Ein erster Entwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes des Bundesministeriums für Verkehr vom 10.9.1993, der eine diesbezügliche Änderung des § 52 Abs. 2 BZRG vorsah, ist bis heute nicht wieder aufgegriffen worden.

Aus diesem Grund bat der Landesbeauftragte im August 1994 unter Darlegung seiner Rechtsauffassung das Ministerium für Wohnungswesen, Städtebau und Verkehr um dessen Rechtsauffassung zu dieser Thematik und um Darstellung der Verwaltungspraxis der Fahrerlaubnisbehörden in Sachsen-Anhalt.

Auf seine Anfrage teilte das Ministerium dem Landesbeauftragten kürzlich mit, daß bezüglich der Verwertungspraxis strafrechtlicher Verurteilungen, die in den beiden o.g. Zentralregistern bereits gelöscht sind, eine unterschiedliche Verfahrensweise bei den Fahrerlaubnisbehörden in Sachsen-Anhalt bestehe. Bei einem großen Teil der Fahrerlaubnisbehörden erfolge keine Verwertung mehr, wenn die Entscheidung länger als 10 Jahren zurückliegt. Andere Fahrerlaubnisbehörden machten von der Ausnahmeregelung des § 52 Abs. 2 BZRG im Rahmen ihres Ermessens längeren Gebrauch.

Über die rechtliche Beurteilung und die Forderung nach Festlegung einheitlicher Verwertungsfristen besteht nach Ansicht des Ministeriums noch Erörterungsbedarf zwischen dem Bundesministerium für Verkehr und den jeweiligen Landesressorts. Im Frühjahr sollen diese Fragen im Bund-Länder-Fachausschuß „Fahrerlaubniswesen“ behandelt werden. Über dessen Ergebnisse soll der Landesbeauftragte informiert werden.

Aus datenschutzrechtlicher Sicht sind für diesen Bereich eindeutige gesetzliche Regelungen zu Aufbewahrungs- und Verwertungsfristen zu fordern. Für die Übergangszeit empfiehlt der Landesbeauftragte dem Ministerium für Wohnungswesen, Städtebau und Verkehr, schon jetzt mit einer Verwaltungsvorschrift die Aufbewahrung und Verwertung von Verurteilungen für Zwecke der Erteilung oder Entziehung einer Fahrerlaubnis einheitlich für Sachsen-Anhalt zu regeln.

31.3 Kontrolle von Kfz-Zulassungs- und Führerscheinstellen

Im Berichtszeitraum wurden durch den Landesbeauftragten drei Straßenverkehrsbehörden kontrolliert.
Bei der stichprobenartigen Überprüfung der Kfz-Zulassungsstellen und der Führerscheinstellen wurden durch den Landesbeauftragten keine schwerwiegenden Verstöße gegen Regelungen zum Datenschutz im Straßenverkehrsgesetz, der Fahrzeugregisterverordnung und der Straßenverkehrszulassungsordnung festgestellt.
Dem gegenüber mußte der Landesbeauftragte die Datensicherheit im technisch-organisatorischen Bereich dieser Stellen in mehrfacher Hinsicht bemängeln. Erhebliche Mängel wurden allerdings nur in einer Straßenverkehrsbehörde vorgefunden.

31.3.1 Überprüfung von Führerscheinstellen

Für die Verarbeitung personenbezogener Daten in der Führerscheinstelle besteht nur eine unzulängliche bereichsspezifische gesetzliche Grundlage. § 10 Abs. 2 StVZO sieht für die Führerscheinstelle lediglich die Pflicht zur Führung

einer namentlich geordneten Kartei über ausgehändigte Führerscheine vor.
Da aber auch andere personenbezogene Daten (Vermerke über Entziehungen, vorläufige Entziehungen, medizinisch-psychologische Gutachten u.ä.) in Führerscheinakten gespeichert werden müssen, sind zur Zeit ergänzend die Bestimmungen des DSG-LSA zu beachten.
Bei der Führung von Führerscheinakten wurden in den überprüften Führerscheinstellen unterschiedliche Verfahren angewandt. Diese reichten von der Führung **eines** Bürgers in verschiedenen Sachakten bis zur zentralen automatisierten Führung der Daten aller Führerscheininhaber im PC.
Als Mangel bei allen Verfahren stellte der Landesbeauftragte das Fehlen von Fristen zur inhaltlichen Sachprüfung (Prüffristen bei Fahrverbot und Sperre zur Wiedererteilung, Aussonderung, Auskunftssperre u.ä.) fest.
Ohne ein solches Wiedervorlageverfahren findet aber die gesetzlich vorgegebene Erforderlichkeitsprüfung (§ 16 Abs. 2 Nr. 2 DSG-LSA) nicht statt.
Unklarheit herrschte vielfach auch über die Zulässigkeit und den inhaltlichen Rahmen von Auskünften aus diesen Akten an Dritte.

Als Ergebnis seiner Kontrollen wies der Landesbeauftragte deshalb auf die Beachtung der §§ 10, 11, 12 und 16 des DSG-LSA hin.
Die Prüfungsergebnisse zeigen deutlich die Notwendigkeit der Schaffung bereichsspezifischer gesetzlicher Grundlagen auch für den Bereich des Führerscheinwesens. Dafür ist aber der Bundesgesetzgeber zuständig.

31.3.2 Überprüfung von Kfz-Zulassungsstellen

Wie bereits einleitend unter Ziff. 31.3 erwähnt bestanden in einem Überprüfungsfall erhebliche Mängel im technisch-organisatorischen Bereich. In diesem Fall war die Straßenverkehrsbehörde in einer ebenerdigen „Holzbaracke“ untergebracht, die in kaum einem Punkt den Anforderungen an ausreichende technische Sicherungsmaßnahmen nach § 6 DSG-LSA entsprach.
Beanstandungspunkte waren hier z.B. verglaste Eingangstüren, einsehbare Diensträume ohne Sicht- und Einbruchsschutz, die noch dazu an einen öffentlichen Parkplatz grenzten. Auch die Zugangstüren der Dienstzimmer bestanden aus sogenannter „Preßpappe“, besaßen aufgeschraubte Türblenden und die von

außen zugänglichen Schließblenden und Aufhängungen dieser Türen waren in keiner Weise einbruchssicher.

In allen Kfz-Zulassungsstellen wurden in nicht verschließbaren Schränken alte Handkarteien aus DDR-Zeiten (Kennzeichen-Kartei, Halter-Kartei, Kfz-Typen-Kartei) festgestellt. Diese alten Dateien dienten Recherchezwecken und enthielten noch vielfach die in der ehemaligen DDR vergebene Personenkennzahl.
Der Landesbeauftragte hat in diesem Zusammenhang darauf hingewiesen, daß bei der Nutzung dieser Altkarteien aus DDR-Zeiten die einschränkenden Bestimmungen der §§ 32 Abs. 3, 34 und 36 DSG-LSA zu beachten und die auf den Karteikarten noch vorhandenen alten Personenkennzahlen entsprechend den Regelungen des Einigungsvertrages (vgl. Anlage I, Kap. II., Sachgebiet C, Abschnitt III Nr. 3) unverzüglich zu löschen sind.

Fehlverhalten mußte der Landesbeauftragte auch bei der Auskunftserteilung an Bürger feststellen. Diesen wurde von den Kfz-Zulassungsstellen aus falschen datenschutzrechtlichen Bedenken oft nicht die sog. einfache Registerauskunft nach § 39 Abs. 1 StVG erteilt. Sie steht jedem Bürger zu, wenn er unter Angabe des Kfz-Kennzeichens oder der Fahrzeug-Identifizierungsnummer darlegt, daß er z.B. die Halterdaten und Name und Anschrift des Versicherers zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr bzw. zur Erhebung einer Privatklage wegen begangener Verstöße im Straßenverkehr benötigt.

Häufiger Fehler beim automatisiert geführten **örtlichen** Fahrzeugregister war die zu lange Speicherung des Datums „Sicherheitsübereignung“. Sie ist nur zeitweise nach § 3 Abs. 2 Nr. 1 der FRV zulässig und muß im Regelfall spätestens nach Abschluß der Zulassung gelöscht werden (§ 44 Abs. 1 i.V. mit § 32 StVG).

Die in den Prüfberichten des Landesbeauftragten aufgezeigten Mängel wurden in allen Fällen behoben.

31.4 Datenschutz bei Bußgeldverfahren

Im zurückliegenden Berichtszeitraum wurden durch den Landesbeauftragten mehrfach Eingaben von Bürgern im Zusammenhang mit einem Ordnungswidrigkeitenverfahren als Folge einer Verkehrsordnungswidrigkeit bearbeitet.
Dabei wurde in einem Fall durch den Landesbeauftragten ein eindeutiger datenschutzrechtlicher Verstoß festgestellt. Dieser betraf den Versand von Bußgeldbescheiden in nicht verschlossenen Briefumschlägen durch das Ordnungsamt einer Stadt.
Das Versandverfahren wurde daraufhin durch das Ordnungsamt umgehend entsprechend den gesetzlichen Bestimmungen im Verwaltungszustellungsgesetz geändert.

Rechtlich schwieriger zu beurteilen ist in bestimmten Fällen die derzeitige Versendungspraxis des Frontfotos "geblitzter" Kraftfahrzeuge an den Kfz-Halter im Rahmen des Anhörungsverfahrens nach § 55 OWiG. Rechtlich verantwortlich und von der zuständigen Behörde im Ordnungswidrigkeitenverfahren heranzuziehen ist grundsätzlich nur der **Fahrer** des Kraftfahrzeuges, deshalb soll das Beweisfoto neben den Kfz-Daten grundsätzlich nur den rechtlich verantwortlichen Fahrer erkennen lassen. Die Praxis zeigt aber, daß auch die ordnungsgemäße Einstellung der Kamera eine Ablichtung von im Kraftfahrzeug mitfahrenden Personen nicht immer verhindern kann. Dieser Umstand stellt für sich gesehen noch keinen Verstoß gegen datenschutzrechtliche Vorschriften dar, soweit das im Einzelfall tatsächlich und technisch nicht vermeidbar ist und deshalb rechtlich keine bewußt beabsichtigte Erhebung der Mitfahrerdaten vorliegt.
Kritisch überdacht werden muß aber die routinemäßige Versendung eines entsprechenden Fotoabzuges an den Kfz-Halter, denn dies stellt rechtlich eine Datenübermittlung von einer öffentlichen Stelle in den privaten Bereich dar. Dazu findet sich weder im OWiG noch im StVG die erforderliche gesetzliche Regelung. Die deshalb ergänzend anzuwendende Vorschrift des § 12 Abs. 1 DSG-LSA läßt aber eine solche Datenübermittlung in den privaten Bereich nur unter ganz bestimmten Voraussetzungen zu, die für die hier besprochenen Fälle meist nicht vorliegen.

Deshalb empfahl der Landesbeauftragte in diesen Fällen als datenschutzgerechte Verfahrensweise die Herstellung und Versendung eines Teilabzuges vom Bildnegativ, der nur den rechtlich verantwortlichen Fahrer zeigt.

Das Ministerium des Innern lehnt in seiner Stellungnahme eine Änderung der bisherigen Praxis ab.
Begründet wird dies mit der Notwendigkeit der Gewährleistung einer zeitgerechten Verfolgung der Ordnungswidrigkeit und dem bevorstehenden Einsatz eines automatisierten Verfahrens der Herstellung des Frontfotos, bei der die Entwicklung des Filmes und die Anfertigung des Bildpositives automatisiert vorgenommen und digitalisiert in den Anhörungsbogen eingedruckt wird.
Außerdem diene das vollständige Foto ggf. der sachgerechten Verteidigung des Betroffenen.
Richtig ist, daß die sachgerechte Verteidigung des Betroffenen (das kann der Halter oder der Fahrer sein) im OWi-Verfahren nicht beeinträchtigt werden darf. Diese wird auch durch den in der Verfahrensakte befindlichen vollständigen Bildabzug und einen Hinweis bei der Übersendung des Teilabzugs an den Halter gewährleistet.
Der Hinweis auf Beschleunigung und Rationalisierung aber geht fehl, denn Grundrechtsverstöße sind so nicht zu rechtfertigen. Die Verwaltung hat sich an Gesetz und Recht zu halten, und unbeteiligte Mitfahrer brauchen sich nicht von einer staatlichen Stelle als Bilddokument an irgendeinen Kfz-Halter versenden zu lassen.

Der Landesbeauftragte sieht deshalb hierzu weiteren Erörterungsbedarf, denn Beispiele in anderen Bundesländern zeigen die Möglichkeit einer datenschutzgerechten Gestaltung dieses Verfahrens.

32. Vermögensgesetz

32.1 Rechtsanwälte als Berater bei den Ämtern zur Regelung offener Vermögensfragen

Ein Bürger beschwerte sich beim Landesbeauftragten über einen Rechtsanwalt, der bei dem Amt zur Regelung offener Vermögensfragen eines Landkreises als

Berater fungierte. Der Petent machte den Vorwurf, der Berater hätte Schreiben der Behörde ohne Vertretungsvollmacht mit dem Zusatz "Rechtsanwalt" unterschrieben und zudem in den Amtsräumen private Rechtsberatungen angeboten und durchgeführt.
Die eingeholten Stellungnahmen und eine Überprüfung vor Ort gaben Anlaß, den Landkreis auf die Rechte und Pflichten des beratenden Rechtsanwaltes, insbesondere auf die strikte Trennung zwischen Beratertätigkeit und privater Tätigkeit als Rechtsanwalt, hinzuweisen.

Auch war es nach den seinerzeit abgeschlossenen Musterverträgen nicht zulässig, daß der beratende Rechtsanwalt eigenständig Entscheidungen mit direkter Außenwirkung für die Behörde traf.

Ein datenschutzrechtlicher Verstoß wurde mit der erforderlichen Sicherheit jedoch nicht festgestellt, so daß der Landesbeauftragte von einer förmlichen Beanstandung absah.

32.2 Datenübermittlung durch die Ämter zur Regelung offener Vermögensfragen

Eine Bürgerin hatte bei einem Amt zur Regelung offener Vermögensfragen die Rückgabe des früher ihren Eltern gehörenden Einfamilienhauses beantragt.
Vom Landesbeauftragten wollte sie wissen, ob das Amt bei der Bearbeitung ihres Antrages berechtigterweise den derzeitigen Verfügungsberechtigten des Hauses Namen und Anschriften aus dem von ihr vorgelegten Erbschein übermittelte.

Nach § 31 Abs. 2 des Gesetzes zur Regelung offener Vermögensfragen (VermG) hat das Amt die Verfügungsberechtigten als betroffene Rechtsträger über die Antragstellung, auf Antrag auch unter Übersendung einer Abschrift des Antrags und seiner Anlagen, zu informieren und zu dem weiteren Verfahren hinzuzuziehen.
Der Landesbeauftragte konnte daher der Petentin mitteilen, daß die Übermittlung der Namen und Anschriften der auf dem Erbschein genannten Personen an die Verfügungsberechtigten keinen Verstoß gegen datenschutzrechtliche Bestimmungen darstellt.

33. Wahlen

33.1 Speicherung des Parteimerkmals bei Unterstützerunterschriften von Kreiswahlvorschlägen

Aufgrund einer Eingabe wurde bei der datenschutzrechtlichen Prüfung festgestellt, daß aus Anlaß der Bundestagswahl 1994 bei einem Wahlamt

- noch Monate nach der Wahl Namen von Unterstützerunterschriften von Kreiswahlvorschlägen gespeichert waren und
- die gespeicherten Daten teilweise an Dritte übermittelt wurden.

Beides war unzulässig und wurde vom Landesbeauftragten formell beanstandet.

Richtig ist, daß die Wahlberechtigung eines jeden Unterstützers eines Wahlvorschlages anhand des Melderegisters festzustellen ist. Und da ein Wahlberechtigter nur **einen** Kreiswahlvorschlag unterzeichnen darf - hat er mehrere Kreiswahlvorschläge unterzeichnet, so ist seine Unterschrift auf allen Kreiswahlvorschlägen ungültig -, ist auch insoweit eine Kontrolle erforderlich.
Dazu dürfen für einen gesetzlich bestimmten Zeitraum vor der Wahl namentliche Aufstellungen (Listenform oder Datei) angefertigt oder eine neutrale Kennzeichnung im Melderegister über die Ausstellung einer Wahlrechtsbestätigung vorgenommen werden. Namensbezogene Hinweise auf die mit dem Vorschlag unterstützte Partei dürfen aber in keinem Fall gespeichert werden.

Diese sich unmittelbar aus dem Gesetz ergebende Rechtslage war seinerzeit allen Kreiswahlleitern auf verschiedenen Wegen mehrfach bekannt gegeben worden.

Der beim Wahlamt festgestellte erste Fehler zog den zweiten nach sich. Weil die erstunterstützte Partei (unzulässigerweise) gespeichert war, erfuhr nunmehr die zweitunterstützte Partei bei der Bekanntgabe von Doppelunterstützungsfällen mehr oder weniger zufällig auch, wen die Wahlberechtigten noch unterstützt hatten.

Auch das stellte einen gesetzlich nicht erlaubten Eingriff in das Grundrecht auf informationelle Selbstbestimmung der davon betroffenen Wahlberechtigten dar.

33.2 Erfassung aller Vorbestraften in den neuen Bundesländern wegen Wahlrechtsausschlüssen

Nur mit Mühe konnte ein wenig sensibler und für die Betroffenen verheerender Gesetzentwurf der Bundesregierung zum Jahreswechsel 1993/1994 noch gestoppt werden. Mit einer unbedachten Änderung des Bundeszentralregistergesetzes wollte die Bundesregierung die Rechtslage dafür schaffen, daß bei den Innenministern der neuen Länder eine komplette Liste aller Vorbestraften des jeweiligen Bundeslandes aus dem Bundeszentralregister vorgelegen hätte. Dabei ging es nur darum, daß die wenigen Straftäter, bei denen die Gerichte auch das Wahlrecht bzw. die Wählbarkeit durch Urteil ausgeschlossen hatten, nicht an den Wahlen des Jahres 1994 teilnahmen. Das war - jedenfalls in Sachsen-Anhalt - viel einfacher und vor allem datenschutzgerechter zu erreichen.

Der Landesbeauftragte konnte sehr schnell mit dem Landeswahlleiter des Landes Sachsen-Anhalt sowie den Ministerien des Innern und der Justiz Einigkeit dahingehend erzielen, daß die schon im Vorgriff auf den Gesetzentwurf vorgesehene Überprüfungsweise im Land Sachsen-Anhalt nicht praktiziert wurde.

Gleichzeitig hatten alle Landesbeauftragten für den Datenschutz der neuen Bundesländer sowie der Bundesbeauftragte für den Datenschutz beim Bonner Gesetzgeber wegen Verstoßes gegen den Verhältnismäßigkeitsgrundsatz und fehlender Erforderlichkeit erhebliche verfassungsrechtliche Bedenken geltend gemacht. Nicht zuletzt aufgrund dieser massiven Einwände hat die Bundesregierung dann den Gesetzentwurf geändert. Die jetzt in den §§ 69 und 70 BZRG enthaltene Lösung der gezielten Selektion unmittelbar beim Bundeszentralregister und die anschließend vorgesehene Übermittlung der entsprechenden Fälle an die für die Führung der Wählerlisten zuständigen Stellen in den Ländern ist datenschutzgerecht.

34. Wasserrecht

In seinem I. Tätigkeitsbericht (S. 161 f) hatte der Landesbeauftragte über mehrere in der parlamentarischen Beratung befindliche Entwürfe eines Wassergesetzes informiert, die seiner Auffassung nach alle den Schutz der personenbezogenen Daten bei der Einsichtnahme in das sogenannte Wasserbuch nicht ausreichend berücksichtigten.
Der Landesbeauftragte hatte deshalb angeregt, das vorgesehene, uneingeschränkte Einsichtsrecht für jedermann in ein Auskunftsrecht umzuwandeln. Ein Anspruch auf Auskunft sollte nur dann nicht bestehen, wenn durch die Auskunft personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden.

Das Wassergesetz für das Land Sachsen-Anhalt (WG LSA) vom 31. August 1993 enthält mit § 190 Abs. 1 ("Auskunftserteilung") eine Vorschrift, die diesen Forderungen nur unpräzise Rechnung trägt, weil Satz 2 ("Die Anforderungen des Datenschutzes sind zu beachten.") zu allgemein formuliert ist. Ein Verweis auf § 12 Abs. 1 Nr. 2 DSG-LSA (Interessenabwägung bei der Datenübermittlung an nichtöffentliche Stellen) wäre hier deutlicher und besser gewesen!

Anlage 1

Organisationsplan Stand: 31.03.1995

Landesbeauftragter für den Datenschutz Sachsen-Anhalt
Herr Kalk

Referat 1	Referat 2	Referat 3
1.1 Grundsatzangelegenheiten, Internationaler Datenschutz, Bildung, Öffentlicher Dienst, Personalvertretung, Landtag, Geschäftsstellenleitung	2.1 Rechtspflege, Strafvollzug, Ordnungswidrigkeitenrecht, Petitionen	3.1 Technik und Organisation des Datenschutzes, Informationstechnik, Verkehr, Raumordnung und Landesplanung
1.2 Hochschulen, Sozialwesen, Gesundheitswesen, Jugendhilfe	2.2 Polizei, Verfassungsschutz, Feuerwehr, Katastrophenschutz, Finanzen	3.2 Technik und Organisation des Datenschutzes, Informationstechnik, Statistik, Vermessungs- und Katasterwesen
1.3 Personenstandswesen, Kultur, Denkmalschutz, Archivwesen, Natur-, Umweltschutz, Wissenschaft und Forschung, Schulen	2.3 Ausländer, Aussiedler, Staatsangehörigkeit, Gewerbeaufsicht, Wehrpflicht, Kommunale Angelegenheiten, Landwirtschaft und Forsten, Wasserrecht, Bau- und Bodenangelegenheiten	3.3 Technik und Organisation des Datenschutzes, Informationstechnik, Medien, Wirtschaft, Handwerk und Gewerbe, Dateienregister, Gleichstellungsfragen
1.4 Verwaltungsangelegenheiten der Geschäftsstelle, Wahlen, Ausweis-, Meldewesen		

Dienstgebäude: Berliner Chaussee 9
39114 Magdeburg

Postanschrift: Postfach 1947
39009 Magdeburg

Telefon: (0391) 81803-0

Telefax: (0391) 81803-33

Anlage 2

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ) vom 26./27. Oktober 1993

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung insbesondere aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

Anlage 3

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Integrierten Verwaltungs- und Kontrollsystem (InVeKoS) (Verordnungen der EWG Nrn. 3508/92 und 3887/92) vom 26./27. Oktober 1993

Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedsstaaten dabei zur Einführung eines "Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)" verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.
Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem "Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.
Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte fordern daher die Datenschutzbeauftragten des Bundes und der Länder,

- ortsunabhängige Überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) nicht für eine flächendeckende Totalüberwachung einzusetzen, sondern auf den von der EG geforderten Stichprobenumfang zu beschränken;
- bei der Nutzung des Kontrollsystems InVeKoS und der darin gespeicherten personenbezogenen Daten den Grundsatz der Verhältnismäßigkeit und insbesondere der Zweckbindung zu beachten;
- nur dezentrale Datenbanken in den einzelnen Bundesländern einzurichten (keine Euro- oder Zentraldatenbank über Landwirte!), und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln;

- zu beachten, daß die EG-Verordnungen zu InVeKoS keine Rechtsgrundlage für eine Erweiterung der Nutzungen enthalten (z.B. zu Kontrollzwecken bei anderen landwirtschaftlichen Förderungsmaßnahmen oder außerhalb des landwirtschaftlichen Bereichs, z.B. zur Besteuerung).

Anlage 4

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zum Ausländerzentralregistergesetz

(gegen die Stimme Bayerns)

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens 8 Millionen Ausländern, die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 02. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden.

Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern - worauf die Entwurfsbegründung hinweist - der Kriminalitätsbekämpfung.

Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen unter denen u.a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen - wenn auch reduzierten - Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

Anlage 5

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 zu Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten von Bund und Länder verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und

- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte "Gesundheitskarten", etwa "Service-Karten" von Krankenversicherungen und privaten Anbietern, "Notfall-Karten", "Apo(theken)-Cards" und "Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen "Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkartentechnik ungleich komplexer und vielfältig nutzbar.

Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt.
So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkartentechnik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller - etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse - mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karteninhabern vorbehält bzw. erleichtert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse ggf. ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die "Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkartentechnik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten - wie den Medizinern - und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest - vorbehaltlich weiterer Punkte - die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.
- Die freiwillige Gesundheitskarte darf nicht - etwa durch Integration auf einem Chip -die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.
- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.
- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung - z.B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung - entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.
- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.
- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

Anlage 6

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zur Informationsverarbeitung im Strafverfahren

(bei Stimmenthaltung Bayerns)

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz - BT-Drucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittlungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren - auch mit Zwangsmitteln - erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.

1.1 Insgesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z. B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z. B. Spurendokumentations- und Recherchesysteme).

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.

In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegriffen werden muß.

Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrunde liegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden - also auch von anderen Staatsanwaltschaften - Auskunft verlangen (§ 161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit - ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens - von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften.

Auf § 78 SGB X ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu "Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 "Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 05./06. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 03. November 1988).

Anlage 7

Entschließung der Datenschutzbeauftragten des Bundes und der Länder zum Entwurf der NADIS-Richtlinien vom 2. Mai 1994

Das von den Verfassungsschutzbehörden des Bundes und der Länder betriebene Verbundsystem NADIS-PZD (Nachrichtendienstliches Informationssystem/Personen-zentraldatei) ist nach den Vorgaben der in Überarbeitung befindlichen NADIS-Richtlinien und der nunmehr erstellten Dateianordnung als Aktenhinweissystem zu qualifizieren. Die NADIS-Richtlinien und die Dateianordnung haben sich hinsichtlich ihres Regelungsgehaltes an den Bestimmungen der Verfassungsschutzgesetze zu orientieren.

Die Datenschutz beauftragten des Bundes und der Länder halten den Entwurf der NADIS-Richtlinien und der Dateianordnung für die Personenzentraldatei für zu weitgehend und fordern deshalb:

- Die in der Personenzentraldatei gespeicherten personenbezogenen Daten sind auf das unerläßlich notwendige Maß zu reduzieren. Eine solche automatisierte Datei darf nach den bindenden Vorgaben des Bundesverfassungsschutzgesetzes nur die Daten enthalten, die für das Auffinden der Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Eine Erweiterung für andere Identifizierungszwecke scheidet somit aus.
  Die Dateianordnung enthält darüber hinaus Arten von Daten, die über den Zweck einer Aktenhinweisdatei hinausgehen.

- Alle Rechtsvorschriften, die für die an dem zu übermittelnden Datensatz beteiligten Verfassungsschutzbehörden maßgeblich sind, sind zu beachten. Die in dem Entwurf der NADIS-Richtlinien enthaltenen Regelungen für die Übermittlung personenbezogener Daten sehen hingegen vor, daß hierfür ausschließlich das Recht der übermittelnden Stelle gelten soll.

- Die Dauer der Speicherung von Protokolldatenbeständen ist einheitlich zu regeln. Eine Differenzierung, ob die ursprünglich in der Personenzentraldatei erfaßte Information infolge Fristablaufs oder aufgrund einer Einzelfallentscheidung gelöscht wurde, erscheint nicht sachgerecht. Außerdem muß sichergestellt sein, daß Protokolldaten, so wie es die Verfassungsschutzgesetze vorsehen, nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage verwendet werden.

- Die Datenschutzbeauftragten sind im Rahmen der Durchführung und Fortentwicklung des Nachrichtendienstlichen Informationssystems frühzeitig zu unterrichten und zu beteiligen. Dies muß insbesondere bei der Vorbereitung von datenschutzrechtlichen Regelungen gelten.

Anlage 8

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zum Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik - EG-Statistikverordnung - (KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings daraufhin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 - Beschluß -).

Gegen den vorgelegten Vorschlag einer **Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik** (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen - insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung - bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können.

Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.

Zugleich sollte EUROSTAT zumindestens einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotenen Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff "statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 - allerdings mit einem anderen Begriffsinhalt - definiert wird. Der Begriff "statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidiarität sollte - ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) - auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag. Dieser gebietet hier, daß - jedenfalls grundsätzlich - die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.

   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z.B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen.

Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

Anlage 9

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu datenschutzrechtlichen Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (Europol)

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit EUROPOL unberührt.

- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, zum Beispiel durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

Anlage 10

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu fehlenden bereichsspezifischen gesetzlichen Regelungen bei der Justiz

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Statt dessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,

- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,

- Übermittlung von Daten aus den bei Gerichten geführten Registern (z.B. Grundbuch) und deren Nutzung durch die Empfänger,

- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz)

- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sog. Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

Anlage 11

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu Vorschlägen zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

   Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll.

Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d. h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

Anlage 12

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zum Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.

- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtsprechung des Bundesverfassungsgerichts sicherzustellen.

Anlage 13

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Kontrolle der Sicherheitsüberprüfungsakten beim Verfassungsschutz vom 26./27. September 1994

Das Ergebnis einer datenschutzrechtlichen Kontrolle von Sicherheitsüberprüfungsakten im Land Mecklenburg-Vorpommern gibt Anlaß zu folgenden Feststellungen:

- Auch die Verfassungsschutzbehörden der neuen Länder dürfen für Zwecke der Sicherheitsüberprüfungen nur Daten verarbeiten und nutzen, die sie zur Erfüllung der ihnen gesetzlich vorgeschriebenen aufgaben tatsächlich benötigen.

- Bürger aus westlichen und östlichen Bundesländern dürfen im Rahmen von Sicherheitsüberprüfungen nicht unterschiedlich behandelt werden.
  Insbesondere sind die Datenschutzbeauftragten der neuen Länder der Auffassung, daß allein die Mitgliedschaft in der SED oder einer der anderen Blockparteien nicht grundsätzlich als sicherheitserheblicher Sachverhalt zu werten ist.

- Datenerhebungen zu Sicherheitsüberprüfungen dürfen nur im Rahmen des SÜG erfolgen.

- die Landesregierungen der neuen Bundesländer werden gebeten, dafür Sorge zu tragen, daß möglichst kurzfristig Sicherheitsüberprüfungsgesetze der Länder verabschiedet werden.

Anlage 14

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Entwurf eines Gesetzes über das Bundeskriminalamt (BKA-Gesetz) - Bundesrats-Drucksache 94/95 vom 9./10. März 1995

Zu den Beratungen des Entwurfs für ein Gesetz über das Bundeskriminalamt erklären die Datenschutzbeauftragten des Bundes und der Länder:
Auch aus Sicht des Datenschutzes ist es zu begrüßen, daß die seit langem überfälligen bereichsspezifischen Regelungen zur bundesweiten polizeilichen Datenverarbeitung insbesondere im polizeilichen Informationssystem (INPOL) nunmehr in das Gesetzgebungsverfahren eingebracht werden. Der Gesetzentwurf enthält im Vergleich zu den Vorentwürfen eine Reihe von Vorschriften, die datenschutzrechtlich positiv zu werten sind.
Hierzu gehören:

- der Verzicht auf die im Vorentwurf vorgesehenen Befugnisse zur sog. "Feststellung des Anfangsverdachts";
- das Erfordernis der Einwilligung für die Speicherung von Daten über Zeugen und mögliche Opfer;
- Übermittlungsverbote bei überwiegenden schutzwürdigen Interessen der Betroffenen oder bei entgegenstehenden gesetzlichen Verwendungsregelungen;
- die Beachtung landesgesetzlicher Löschungsfristen.

Andererseits begegnet der Gesetzentwurf jedoch nach wie vor gewichtigen Bedenken, da er tiefe Eingriffe in die Rechte von Betroffenen ermöglicht, deren Voraussetzungen und Reichweite unklar oder nicht durch überwiegende Interessen der Allgemeinheit gerechtfertigt sind. Dies gilt insbesondere für

- die Verwendung des Begriffs der Straftaten von erheblicher Bedeutung ohne Definition, um welche Tatbestände es sich handelt, weil damit nicht mehr voraussehbar ist, wann die an diesen Begriff anknüpfenden Eingriffsbefugnisse zur Datenverarbeitung eröffnet sind;
- die Befugnisse der Zentralstelle zu selbständigen Datenerhebungen und Übermittlungen bis hin zum automatisierten Datenverbund mit ausländischen und zwischenstaatlichen Stellen ohne Einvernehmen mit den jeweils verantwortlichen Länderpolizeien;

- die unklare Abgrenzung der Datenverarbeitungsbefugnisse im Hinblick auf die unterschiedlichen Befugnisse zur Strafverfolgung, Gefahrenabwehr, Verhütung von Straftaten und Vorsorge für künftige Strafverfolgung sowie die fehlende klare Zweckbindungs- und Zweckänderungsregelung;
- die Befugnis zur verdeckten Datenerhebung aus Wohnungen ohne eindeutige Begrenzung auf den Schutz gefährdeter Ermittler.

Die Datenschutzbeauftragten fordern den Gesetzgeber auf, die Schwachstellen des Entwurfs auszuräumen. Insbesondere fordern sie klare verfassungskonforme Regelungen zur Auskunftserteilung an Betroffene und der Prüfrechte für INPOL-Daten dahingehend, daß die Datenschutzkontrollrechte bei der datenschutzrechtlichen Verantwortung der Stellen anknüpfen, die die Speicherung im INPOL-System selbst vornehmen oder veranlassen.

Anlage 15

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu Aufbewahrungsbestimmungen und Dateiregelungen im Justizbereich vom 9./10. März 1995

Bisher ist der Gesetzgeber im Bereich der Justiz den verfassungsrechtlichen Forderungen nach ausreichenden normenklaren Regelungen über die Aufbewahrung von Akten und die Speicherung personenbezogener Daten in Dateien nicht nachgekommen. So enthalten z.B. die bislang bekannt gewordenen Entwürfe zu einem Strafverfahrensänderungsgesetz nur unzureichende Generalklauseln. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder[*)] erklärt deshalb:

1. Aufbewahrung, Aussonderung und Vernichtung der Akten und die Speicherung personenbezogener Daten in Dateien im Bereich der Justiz müssen nach den Grundsätzen des Bundesverfassungsgerichts im Volkszählungsurteil für die Gerichte, Staatsanwaltschaften und Strafvollzugsbehörden gesetzlich geregelt werden, wobei sich die Aufbewahrungsdauer am Recht auf informationelle Selbstbestimmung und am Zweck der Speicherung zu orientieren hat.
   Hierbei hat der Gesetzgeber die grundlegenden Entscheidungen zur Aufbewahrungsdauer selbst zu treffen. Aufgrund einer hinreichend konkreten Verordnungsermächtigung können die Einzelheiten durch Rechtsverordnung bestimmt werden.
2. Die derzeit bestehenden Aufbewahrungsfristen sind konsequent zu vereinfachen und zu verkürzen. Soweit geboten sind Verkürzungen vorzunehmen.
3. Die derzeit geltende generelle 30-jährige Aufbewahrungsfrist für Strafurteile und Strafbefehle mit der Folge der umfassenden Verfügbarkeit der darin enthaltenen Informationen ist nicht angemessen. Bei der Bemessung der Aufbewahrungsfrist von Strafurteilen und Strafbefehlen sowie für die Bestimmung des Zeitpunkts der Einschränkung der Verfügbarkeit ist vielmehr nach Art und Maß der verhängten Sanktionen zu differenzieren.
   Bei der Festlegung des Beginns der Aufbewahrungsfrist sollte - abweichend von der bisherigen Praxis, nach der es auf die Weglegung der Akte ankommt - regelmäßig auf den Zeitpunkt des Eintritts der Rechtskraft der ergangenen gerichtlichen Entscheidung abgestellt werden.

Ergeht keine rechtskraftfähige Entscheidung, so sollte die Aufbewahrungsfrist mit dem Erlaß der Abschlußverfügung beginnen.

4. Wird der Akteninhalt auf Bild- oder Datenträgern, die an die Stelle der Urschrift treten, aufbewahrt, so sind gleichwohl unterschiedliche Löschungsfristen für einzelne Aktenteile zu beachten. Aus datenschutzrechtlicher Sicht sind Datenträger zu wählen, die eine differenzierte Löschung gewährleisten. Ist bei Altbeständen eine teilweise Aussonderung technisch nicht möglich oder nur mit unverhältnismäßigem Aufwand zu bewerkstelligen, so hat eine Sperrung der an sich auszusondernden Teile zu erfolgen.
5. Sind in einer Akte Daten mehrerer beteiligter Personen gespeichert, so ist eine Sperre hinsichtlich solcher Aktenteile, die einzelne beteiligte Personen betreffen, vorzusehen, wenn diese Aktenteile eigentlich ausgesondert werden müßten, aus praktischen Gründen aber keine Vernichtung erfolgen kann.
6. Bei Freisprüchen und Einstellungen des Verfahrens wegen Wegfalls des Tatverdachts ist dafür Sorge zu tragen, daß ein Zugriff auf die automatisiert gespeicherten Daten nur noch zu Zwecken der Aktenverwaltung erfolgen kann.
7. Für die Daten von Nebenbeteiligten (z.B. Anzeigeerstatter, Geschädigte) ist eine vorzeitige Löschung vorzusehen. Hinsichtlich der Hauptbeteiligten sollte eine Teillöschung der Personen- und Verfahrensdaten stattfinden, sobald die vollständigen Daten zur Durchführung des Verfahrens nicht mehr erforderlich sind.
8. Soweit Daten verschiedener Gerichtszweige oder verschiedener speichernder Stellen in gemeinsamen Systemen verarbeitet werden, ist durch rechtliche, technische und organisatorische Maßnahmen sicherzustellen, daß die Zweckbindung der gespeicherten Daten beachtet wird.

*) Bei Stimmenthaltung von Hamburg

Anlage 16

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz bei elektronischen Mitteilungssystemen vom 9./10. März 1995

Es ist damit zu rechnen, daß in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche bedeutsame Informationen und insbesondere personenbezogene Daten über Netze ausgetauscht werden.
Die zunehmende Nutzung von elektronischen Mitteilungssystemen (Electronic-Mail, Dokumentenaustausch über Datenfernübertragung, Message Handling Systems MHS/X.400) hat zur Folge, daß Bedrohungen wie Verlust von Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit verschärft werden, weil Unbefugte Zugriffe auf Daten und Programme erhalten können und die Übertragungswege vom Kommunikationspartner nicht sicher zu kontrollieren sind. Deshalb ist beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In diesem Zusammenhang gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information durch eine Vielzahl umfassender aufeinander abgestimmter Sicherheitsmaßnahmen an Bedeutung.
Die Datenschutzbeauftragten des Bundes und der Länder fordern, daß den folgenden Sicherheitsaspekten beim Einsatz von elektronischen Mitteilungssystemen Rechnung getragen wird:

1. Authentizität von Benutzern, Nachrichten und Systemmeldungen

Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders, der Nachricht sowie der an ihn gerichteten Systemmeldungen (z. B. Empfangs- und Weiterleitungsbestätigungen, Sendeanforderungen, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. Vertraulichkeit von übertragenen Daten

Für alle Arten von Daten in elektronischen Mitteilungssystemen - Nachrichten sowie Verkehrs- und Verbindungsdaten - muß die Vertraulichkeit gewahrt bleiben. Sie ist durch geeignete Maßnahmen, z.B. kryptografische Verfahren, sicherzustellen.

3. Integrität von Nachrichten und Meldungen

Es ist zu gewährleisten, daß bei Speicherung und Weiterleitung von Daten keine unbefugte, unerkannte Veränderung erfolgen kann.

4. Fälschungssichere Kommunikationsnachweise

Die für die Anerkennung einer elektronischen Kommunikation erforderlichen fälschungssicheren Sende-, Empfangs- und Übertragungsnachweise müssen dem Anwender auf Wunsch zur Verfügung stehen.

5. Ausschluß von Kommunikationsprofilen

Die Erstellung von Kommunikationsprofilen muß verhindert werden. Gespeicherte Protokollierungsdaten dürfen nur zu Zwecken des Datenschutzes und der Datensicherung (§§ 14 Abs. 4, 31 BDSG bzw. landesgesetzliche Regelungen) verwendet werden.

Empfehlungen zum Einsatz von elektronischen Mitteilungssystemen:

Zum sicheren Einsatz von elektronischen Mitteilungssystemen sind als Grundschutzmaßnahmen folgende Empfehlungen zu beachten.

1. Grundsätzlich sind nur solche Produkte einzusetzen, die die Sicherheitsfunktionen der X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme - insbesondere solche, die noch auf Empfehlungen von 1984 basieren -, sollen künftig durch geeignete Zusatzprodukte hinsichtlich ihrer Sicherheit verbessert oder durch neuere Softwareversionen ersetzt werden.
2. Bei Übertragung von personenbezogenen Daten ist eine Verschlüsselung vorzusehen. Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z.B. DES, IDEA) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein. Verschlüsselungskomponenten sind durch technische, bauliche und organisatorische Maßnahmen vor dem Zugriff Unbefugter zu schützen.
3. Zur Absicherung der Integrität der Daten sollte auf Verfahren der "elektronischen Unterschrift" zurückgegriffen werden.
4. Nach Möglichkeit ist die Funktion des Systemverwalters von der des Netzwerkverwalters - insbesondere der Verwaltung des elektronischen Mitteilungssystems - aus Sicherheitsgründen zu trennen.

5. Es ist grundsätzlich separat administrierbare Hard- oder Software - z.B. in Form eines Kommunikationsservers - für das elektronische Mitteilungssystem vorzusehen.
6. Bei Verwendungen von öffentlichen Übertragungswegen sind die vorhandenen Sicherheitsmechanismen dieser Netze, z.B. geschlossene Benutzergruppen, Rufnummernidentifikation, Teilnehmerzeichengabe und automatische Rückruffunktion zur Abwehr des Zugriffs durch externe zu nutzen.
7. Zur Beweissicherung einer stattgefunden Kommunikation sollte die eingesetzte Software folgende Funktionen beinhalten:
   - Zustellung/Empfangsnachweise
   - Sende/Empfangsübergabenachweise

Anlage 17

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur automatischen Erhebung von Straßenbenutzungsgebühren vom 9./10. März 1995

Gegenwärtig werden Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren in mehreren Versuchsfeldern erprobt. Sie können im Rahmen der weiteren Entwicklung zu zentralen Komponenten umfassender Verkehrstelematiksysteme (z.B. Verkehrsinformation und -leitung) werden.
Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern, erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, daß Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfaßt, sich möglichst frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig, elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren wie z. B. die Vignette einzubeziehen.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, daß der Grundsatz der datenschutzgerechten Ausgestaltung von Systemen zur automatischen Erhebung von Straßenbenutzungsgebühren von allen Beteiligten am Feldversuch auf der BAB A 555 akzeptiert wird. Zur Umsetzung dieses Grundsatzes fordern die Datenschutzbeauftragten:

- Der Grundsatz der "datenfreien Fahrt" muß auch künftig gewährleistet sein. Über Verkehrsteilnehmer, die ordnungsgemäß bezahlen, dürfen keine Daten erhoben oder verarbeitet werden, die die Herstellung eines Personenbezugs ermöglichen. Es sind ausschließlich solche Zahlungsverfahren anzuwenden, bei denen die Abrechnungsdaten nur dezentral beim Verkehrsteilnehmer gespeichert werden. Die Verkehrsteilnehmer dürfen jedoch nicht gezwungen werden, einen lückenlosen Nachweis über ihre Bewegungen zu führen.

- Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Möglichkeit einer flächendeckenden Kontrolle ist von vornherein technisch und rechtlich auszuschließen. Die Gebührenkontrolle ist so zu gestalten, daß die Identität des Verkehrsteilnehmers nur dann aufgedeckt wird, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Gebühren nicht entrichtet worden sind.
- Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Verkehrsteilnehmer durchschaubar sein. Der Verkehrsteilnehmer muß jederzeit über sein Guthaben, die Abbuchung und den eventuellen Kontrollvorgang informiert sein.
- Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, daß sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

Die hierbei anzuwendenden Verfahren wären gesetzlich abschließend vorzugeben. Dabei ist sicherzustellen, daß anfallende personenbezogene Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen. Ferner ist zu gewährleisten, daß Betreiber derartiger Systeme - unabhängig von ihrer Rechtsform - einer Datenschutzkontrolle nach einheitlichen Kriterien unterliegen. Die Bundesregierung wird aufgefordert, bei der anstehenden internationalen Normierung elektronischer Mautsysteme die datenschutzrechtlichen Anforderungen durchzusetzen.

Anlage 18

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Datenschutz bei Wahlen vom 9./10. März 1995

Bei der Durchführung von Wahlen haben sich Probleme bei der Verarbeitung personenbezogener Daten ergeben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu die folgende Entschließung[*)] gefaßt:

1. Durchführung von Wahlstatistiken

Diejenigen Wahlberechtigten, in deren Wahlbezirk eine repräsentative Wahlstatistik durchgeführt werden soll, sind bereits mit der Wahlbenachrichtigung hierüber zu informieren. In allgemeiner Form ist auch im Wahllokal ein gut sichtbarer Hinweis auf die Einbeziehung in die Wahlstatistik anzubringen.

Die Statistik sollte nur in solchen Wahlbezirken durchgeführt werden, in denen jede Geschlechts- und Altersgruppe wenigstens so viele Wahlberechtigte aufweist, daß das Wahlgeheimnis mit Sicherheit gewahrt bleibt. Das Kriterium ist vom Landeswahlleiter vor der Festlegung der Auswahlbezirke zu prüfen. Gegebenenfalls sind ungeeignete Wahlbezirke auszutauschen.

Die Auszählung der Wahlberechtigten und der Wahlbeteiligung auf der Grundlage der Wählerverzeichnisse sollte durch den Wahlvorstand erfolgen, während die statistische Auszählung der Stimmzettel durch die jeweils für die Durchführung der Statistik zuständige Stelle vorzunehmen ist.

Untersuchungen, bei denen Angaben über die Wahlbeteiligung oder die Stimmabgabe aus verschiedenen Wahlen einzelfall- und personenbezogen zusammengeführt werden, gefährden das Wahlgeheimnis und sind daher unzulässig.

2. Auslegung von Wählerverzeichnissen

Durch die Einsicht in das Wählerverzeichnis besteht nach der jetzigen Rechtslage die Gefahr, daß Daten sowohl von Bürgern, über die in Melderegistern eine Auskunftssperre eingetragen ist, als auch von Bürgern, die in einer speziellen sozialen Situation leben (z.B. Justizvollzugsanstalten, Frauenhäuser, psychiatrische Kliniken, Obdachlose), offenbart werden.

Um einerseits die Kontrollmöglichkeit durch die Öffentlichkeit im Vorfeld einer Wahl weiterhin zu gewährleisten, andererseits die datenschutzrechtlichen Belange der genannten Betroffenen zu wahren und dem Mißbrauch einer Adreßrecherche vorzubeugen, fordern die Datenschutzbeauftragten des Bundes und der Länder, daß bei allen Wahlen

- entweder in den öffentlich ausliegenden Wählerverzeichnissen nur Name, Vorname und Geburtsdatum der Wahlberechtigten aufgeführt werden
- oder aber bei Wiedergabe der Adressen im Wählerverzeichnis nur Auskünfte zu bestimmten Personen an den Auskunftssuchenden erteilt werden, wenn er vorher die Adresse dieser Person angegeben hat.

Im übrigen sind Daten von Bürgern, für die in Melderegistern eine Auskunftssperre eingetragen ist, im Wählerverzeichnis nicht zu veröffentlichen.

3. Gewinnung von Wahlhelfern

Bei der Gewinnung von Wahlhelfern sind folgende Grundsätze zu beachten:
Es dürfen nur die zur Bestellung erforderlichen Daten, wie Name, Vorname und Wohnanschrift, erhoben werden. Die Betroffenen sind über den Zweck der Datenerhebung und die weitere Datenverarbeitung umfassend zu unterrichten.
Über die Abwicklung der jeweiligen Wahl hinaus dürfen die Daten der Wahlhelfer in einer Wahlhelferdatei nur gespeichert werden, wenn sie dieser Speicherung nicht widersprochen haben. Die Wahlhelfer sind auf ihr Widerspruchsrecht hinzuweisen.
Beschäftigtendaten dürfen nur auf freiwilliger Basis übermittelt werden, sofern nicht eine besondere Rechtsvorschrift die Übermittlung zuläßt. Im Falle der Freiwilligkeit muß es den Beschäftigten möglich sein, selbst die Meldung unmittelbar gegenüber der Wahlbehörde abzugeben. Nach Gründen, die einer Übernahme des Ehrenamtes entgegenstehen, darf erst im förmlichen Verfahren durch die Wahlbehörde gefragt werden.

4. Erteilung von Wahlscheinen

Die in den Wahlordnungen des Bundes und der Länder enthaltene Regelung, nach der die Antragstellung für die Erteilung eines Wahlscheines auf einem Vordruck zu begründen ist und der Grund gegenüber der Gemeinde glaubhaft gemacht werden muß, ist aus datenschutzrechtlicher Sicht unverhältnismäßig.

Da sich aus der geforderten Differenzierung der Begründung keine unterschiedlichen Rechtsfolgen ableiten, ist diese entbehrlich. Es genügt in der Antragstellung eine Erklärung des Wahlberechtigten, daß er am Tag der Wahl aus wichtigem Grund das für ihn zuständige Wahllokal nicht aufsuchen kann.

*) Bei Gegenstimme von Baden-Württemberg zu Nr. 4.
Enthaltung von Bayern zu Nr. 2 und von Sachsen-Anhalt und Rheinland-Pfalz zu Nr. 4

Anlage 19

§ 6 DSG-LSA	Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt informiert: **Technische und organisatorische Maßnahmen**	

Dienstanweisung zum Datenschutz und zur Datensicherung

In einer Dienstanweisung zum Datenschutz und zur Datensicherung bei der Verarbeitung und Nutzung personenbezogener Daten empfiehlt es sich, folgende Punkte zu berücksichtigen:

- **Begriffserläuterungen**
  z.B. personenbezogenes Datum; Dateibegriff (automatisiert, nicht-automatisiert); Erheben; Verarbeiten (Speichern, Verändern, Übermitteln, Sperren, Löschen); Nutzen; Anonymisieren; speichernde Stelle; Dritter

- **Ziel, Geltungsbereich und gesetzliche Grundlage**
  der Dienstanweisung selbst sowie für das Erheben und Verarbeiten personenbezogener Daten durch die Behörde (Beachte: spezialgesetzliche Grundlage geht dem DSG-LSA vor, § 3 Abs. 3 DSG-LSA)

- **Zuständigkeit innerhalb der Behörde**
  Aufgaben der einzelnen Organisationseinheiten der Behörde (z.B. der Ämter des Landkreises; Abteilung; Dezernat) bei der Durchführung des Datenschutzes aufführen und ggf. näher erläutern (z.B. Verantwortlichkeit für die Auskunftserteilung, die Datensicherheit, Beschaffung von Hard- und Software, Test und Freigabe von Programmen, Meldungen zum Dateienregister)

- **Technische und organisatorische Maßnahmen**
  - gemäß § 6 Abs. 1 DSG-LSA für **jede Form** der Datenverarbeitung oder -nutzung in entsprechender Abwägung zwischen dem Aufwand und dem angestrebten Schutzzweck der Daten (ausführliche Darlegung in den VV zum § 6 DSG-LSA),
  - gemäß § 6 Abs. 2 DSG-LSA zusätzlich bei **automatisierter Verarbeitung**, wie z.B.:
    - Regelungen zur Zugangskontrolle in Diensträumen mit Informationstechnik
    - Zugriffskontrolle (Paßwortgestaltung/Abschottung der Datenbereiche)
    - Handhabung von Datenträgern mit personenbezogenen Daten (Nachweisführung; Quittierung)
    - regelmäßige Datensicherung und entsprechende verschluß- und feuersichere Aufbewahrung der Sicherungsdisketten bzw. -bänder (z.B. im Data-Safe)
    - Protokollierung der Datenübermittlungen

- **Behördlicher Datenschutzbeauftragter:**
  Stellung, Aufgaben, Befugnisse (siehe Ziff. 14.2.8 VV-DSG-LSA)

Anlage 20

§ 6 DSG-LSA	Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt informiert: **Technische und organisatorische Maßnahmen**	

Klassifizierung personenbezogener Daten nach ihrer Schutzwürdigkeit

Die folgende Klassifizierung der personenbezogenen Daten nach ihrer Schutzwürdigkeit stellt eine Empfehlung dar, die die Auswahl technischer und organisatorischer Maßnahmen gem. § 6 Abs. 1 DSG-LSA erleichtern soll.
Kriterien für die Schutzwürdigkeit personenbezogener Daten können der Grad der Sensibilität und die Menge der gespeicherten personenbezogenen Daten sein. Der Grad der Sensibilität kann z. B. aus den möglichen Folgen bei der Offenbarung der personenbezogenen Daten des Betroffenen abgeleitet werden.
Die folgende Einteilung entbindet die Behörde/das Amt nicht davon, im jeweiligen Einzelfall den Umfang der entsprechenden technischen und organisatorischen Maßnahmen auf ihre Erforderlichkeit hin zu prüfen.

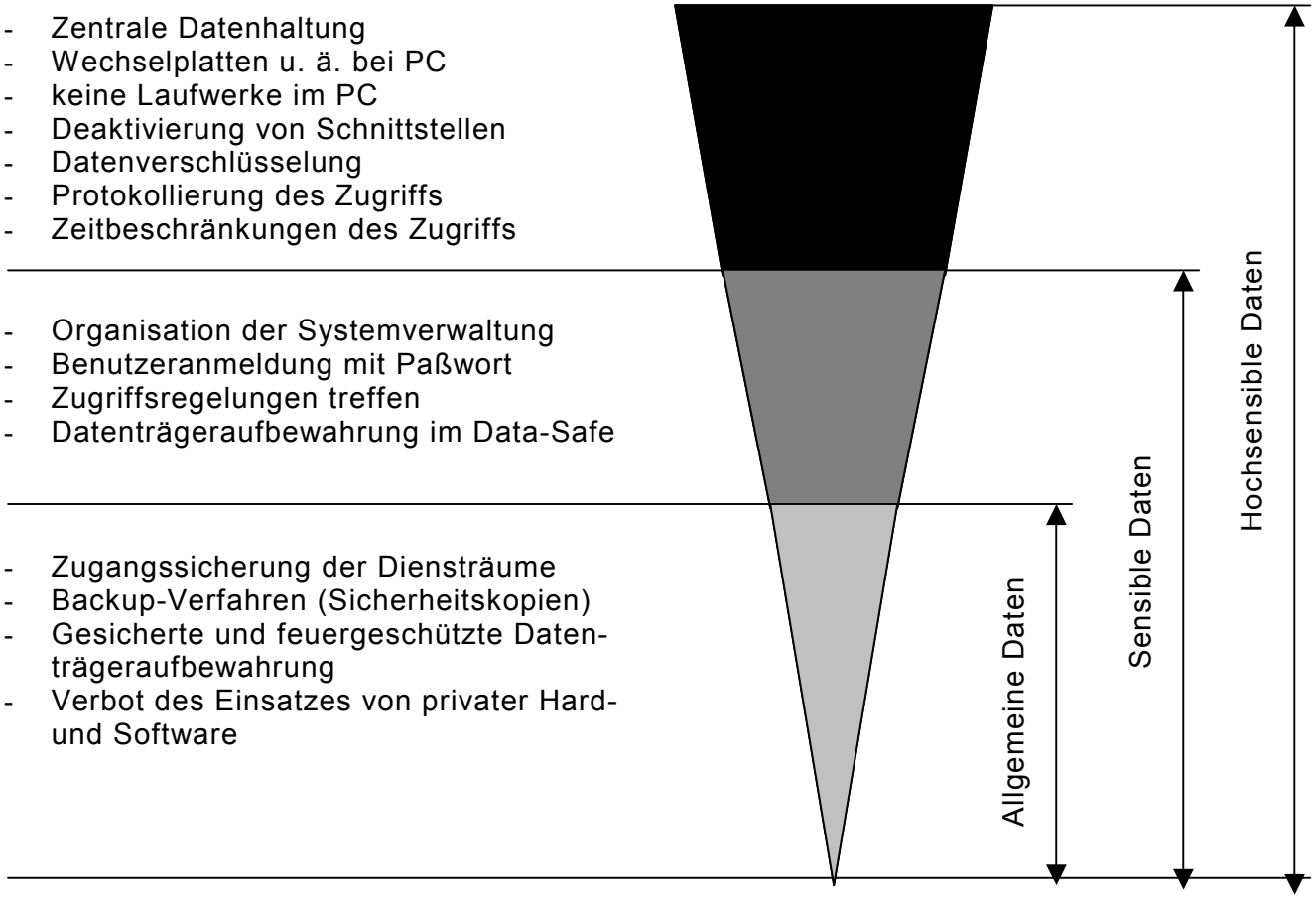
- **Allgemeine Daten**
  - Keine besondere Beeinträchtigung des Betroffenen bei Offenbarung
  - für jedermann zugängliche Daten
    z.B. Öffentliche Register, Adreß- oder Branchenbücher, Benutzerkataloge in Bibliotheken

- **Sensible Daten**
  - Beeinträchtigung des Betroffenen bei Offenbarung der personenbezogenen Daten in seiner gesellschaftlichen Stellung
  - Gefährdung wirtschaftlicher Verhältnisse bei Offenbarung personenbezogener Daten
  - Kenntnisnahme nur bei berechtigtem Interesse
    z.B. halböffentliche Register (nur beschränkt einsehbar), Grundbuchdaten, allgemeine Meldedaten, Archivdaten, Geschäfts- und Vertragsbeziehungen; Mitgliedschaften; Mietverhältnis

- **Hochsensible Daten**
  - Gesetzlich besonders geschützte Daten (Steuerdaten; Personaldaten; Sozialdaten)
  - Gefahr für Leib und Leben (Zeugenschutz)

- **Fundstellen:**
  DSG-LSA vom 12.03.1992 (GVBl. LSA S. 152)
  VV-DSG-LSA vom 14.10.1993 (MBl. LSA S. 2485)

Mögliche Schutzmaßnahmen in Abhängigkeit vom Grad der Sensibilität der personenbezogenen Daten



Anlage 21

§ 8 DSG-LSA	Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt informiert: **Auftragsdatenverarbeitung**	

Für die Verarbeitung oder Nutzung personenbezogener Daten im Auftrag empfiehlt es sich, folgende Punkte bei der Vertragsgestaltung zu berücksichtigen:

- **Grundlagen der Vertragspartner:**
  - Umfang und Grenzen der übertragenen Tätigkeiten
  - schriftliche Auftragserteilung
  - Beachtung der rechtlichen Verantwortlichkeit des Auftraggebers

- **Vertragsinhalt:**
  - Vertragsdauer, Kündigungsfrist, Vertragsstrafe, Haftungsregelungen
  - Verpflichtung der Vertragsparteien zur Anzeige von Veränderungen
  - Regelung bei vertraglichen „Schwebezuständen“ (z.B. Konkurs, Fusion)

- **Pflichten und Rechte des Auftraggebers:**
  - Prüfung der Zulässigkeit einer Auftragsdatenverarbeitung (z.B. Teilverbot § 80 SGB X)
  - Sorgfältige Auswahl des (zuverlässigen) Auftragnehmers
  - Weisungs-, Prüfungs- und Kontrollrechte
  - Art und Weise der Datenübergabe, Programmfreigabe
  - Regelungen über den Verbleib der personenbezogenen Daten bei Beendigung des Auftragsverhältnisses
  - Verpflichtung des Auftragnehmers zur Einhaltung der Bestimmungen des DSG-LSA, wenn auf den Auftragnehmer das DSG-LSA keine Anwendung findet

- **Pflichten und Rechte des Auftragnehmers:**
  - Verarbeitung, insbesondere die Datenübermittlung an Dritte nur nach Weisung des Auftraggebers
  - Beauftragung von Subunternehmer nur nach schriftlicher Zustimmung des Auftraggeber
  - Sicherstellung der technischen und organisatorischen Maßnahmen zur ordnungsgemäßen Absicherung der Verarbeitung personenbezogener Daten entsprechend den gesetzlichen Vorschriften (§ 6 DSG-LSA; Pkt. 6 VV-DSG-LSA)
  - Hinweispflicht des Auftragnehmers in § 8 Abs. 3 DSG-LSA

- **Besondere Vereinbarungen:**
  - Prüfungs- und Kontrollrechte durch den Landesbeauftragten für den Datenschutz bei privaten Auftragnehmern gem. § 8 Abs.6 DSG-LSA
  - Verpflichtung auf datenschutzrechtliche Bestimmungen (z.B. nicht-öffentlicher Auftragnehmer - Datengeheimnis)

Sind auf den Auftragnehmer die Vorschriften des Gesetzes nicht anwendbar, so besteht für den Auftraggeber eine **Meldepflicht** gegenüber dem Landesbeauftragten gem. § 8 Abs. 6 DSG-LSA.

Anlage 22

Schutz Unbeteiligter bei der Übermittlung personenbezogener Daten aus Personalakten und -dateien an die Gerichte

Bekanntmachung des Landesbeauftragten für den Datenschutz
vom 28. Juli 1994 - 15/3 -

In nicht wenigen Bereichen der unmittelbaren und mittelbaren Landesverwaltung findet z.Zt. eine Neuorganisation und ein damit verbundener Personalum- und -abbau statt. Die für die Durchführung dieser Maßnahmen verantwortlichen Personaldienststellen haben dabei die nicht ganz leichte Aufgabe, die Entscheidungen durch das Zusammenstellen vieler sensibler persönlicher Einzelangaben der betroffenen Mitarbeiterinnen und Mitarbeiter vorzubereiten. Gesetzgeber und Gerichte verlangen auch vom öffentlichen Arbeitgeber die soziale Ausgewogenheit jeder einzelnen Kündigung. Nicht selten werden dann in den Kündigungsschutzprozessen vor den Arbeitsgerichten, aber auch bei den sog. Konkurrentenklagen vor den Verwaltungsgerichten, Personaldaten anderer, nicht am Prozeß beteiligter Bediensteter Gegenstand prozessualer Erörterung.

Sowohl die personalführende Dienststelle als auch die angerufenen Gerichte haben dabei das Grundrecht auf informationelle Selbstbestimmung (Art. 6 Abs. 1 LVerf) und das ergänzend zu den einschlägigen prozeßrechtlichen Vorschriften geltende Gesetz zum Schutz personenbezogener Daten der Bürger zu beachten (vgl. § 3 Abs. 1 Satz 1 und Abs. 3 Satz 1 DSG-LSA).
Dem Landesbeauftragten sind mehrere Einzelfälle bekannt geworden, die Unsicherheiten und Fehler beim Umgang mit personenbezogenen Daten unbeteiligter Dritter erkennen lassen.

Der Landesbeauftragte gibt deshalb unter Bezugnahme auf § 22 Abs. 4 Satz 1 DSG-LSA folgende Empfehlungen zur Beachtung des Datenschutzes:

1. Dem Schutz der Persönlichkeit kommt im Bereich der Personalakten- und Personaldateiführung besondere Bedeutung zu. Dem hat der Bundesgesetzgeber für das Rahmenrecht dadurch entsprochen, daß er die Vorschriften der §§ 56 bis 56f BRRG

mit Wirkung vom 1. Januar 1993 neu geregelt hat. Diese Vorschriften bedürfen zwar noch der Umsetzung durch den Landesgesetzgeber, doch stellen Sie bereits heute einen beachtlichen Orientierungsrahmen dar, der jedenfalls nicht mehr überschritten werden darf. Die personalbearbeitenden Dienststellen müssen sich deshalb mit diesen Vorschriften vertraut machen und bereits im vorgerichtlichen Streitverfahren die dort gezogenen Grenzen beim Akteneinsichtsrecht und bei der Übermittlung personenbezogener Daten im Auskunftswege berücksichtigen.

Ist eine Klage beim Arbeitsgericht oder beim Verwaltungsgericht anhängig, gelten für den Umfang der Vorlagepflicht von Unterlagen bzw. der Erteilung von Auskünften die bereichsspezifischen Vorschriften in den Prozeßordnungen, insbesondere § 56 Arbeitsgerichtsgesetz bzw. § 99 Verwaltungsgerichtsordnung. Danach obliegt es zunächst dem Gerichtsvorsitzenden, durch prozeßleitende Verfügungen die Vorlage entsprechender Unterlagen (Personalakten, Vergleichstabellen) anzuregen oder die gesetzliche Vorlagepflicht zu präzisieren. In keinem Fall sollte die personalaktenführende Stelle personenbezogene Unterlagen unbeteiligter Dritter ohne Aufforderung des Gerichts und ohne dessen Bezugnahme auf eine eindeutige Rechtsgrundlage vorlegen.
Auch im Kündigungsschutzprozeß vor dem Arbeitsgericht gilt die Parteiherrschaft, d.h. die Prozeßparteien bestimmen weitgehend selbst, was Prozeßgegenstand wird und wie der Prozeß verläuft. Die dem Arbeitgeber obliegende Darlegungslast (§ 1 Abs. 3 Satz 1, 2. Halbsatz KSchG) verpflichtet nicht zur personenbezogenen Angabe namentlich benannter Vergleichsfälle, sondern verlangt die zahlenmäßig aufgeschlüsselte Darlegung der Ausgewogenheitskriterien, wie Angaben über das Alter, die Betriebszugehörigkeitsdauer und eventuelle Unterhaltsverpflichtungen. Soweit unter Berufung auf anderslautende Urteile und Kommentierungen vereinzelt auch personenbezogene Angaben gefordert werden, ist darauf hinzuweisen, daß die Urteile weitgehend überholt sind, weil sie zeitlich vor der Entscheidung des Bundesverfassungsgerichts vom 15. Dezember 1983 (BVerfGE 65,1) zum Grundrecht auf informationelle Selbstbestimmung liegen. Die Vorschriften des Kündigungsschutzgesetzes sind jetzt verfassungskonform anzuwenden.
Keine Vorlagepflicht des Arbeitgebers besteht auch insoweit, als er für seine Entscheidung auf freiwilliger Basis von den unbeteiligten Dritten mehr persönliche Auswahlkriterien erhalten hat, als nach der Rechtsprechung des Bundesarbeitsgerichts erforderlich sind.

Auch in den Fällen, in denen das Gericht die Vorlage personenbezogener Unterlagen Dritter oder entsprechende Auskünfte über ihre Daten fordert, sollte die personalführende Dienststelle das Gericht unter Hinweis auf das Grundrecht auf informationelle Selbstbestimmung um Möglichkeiten der nur eingeschränkten Vorlage bitten. So reichen z.B. im Fall einer Konkurrentenklage beim Verwaltungsgericht im Regelfall Ausbildungs- und Verwendungsnachweise und die entsprechenden Leistungsbeurteilungen der Mitbewerber - nur ausnahmsweise dürfte die Vorlage der gesamten Personalakte erforderlich werden.

2. Eine sorgfältige Vorabprüfung zum Schutz der unbeteiligten Dritten ist auch deshalb geboten, weil die einmal bei Gericht vorgelegten personenbezogenen Unterlagen nach den Prozeßvorschriften für alle Prozeßbeteiligten praktisch uneingeschränkt zugängig sind (vgl. § 46 Abs. 2 ArbGG i.V. mit § 299 ZPO, § 100 VwGO).
   Müssen Unterlagen Dritter vorgelegt werden, so sollte das Gericht von der vorlegenden Behörde für den Fall der Übermittlung dieser Daten an die anderen Prozeßbeteiligten gebeten werden, eine Zweckbindungserklärung nach § 12 Abs. 4 Satz 1 DSG-LSA auszusprechen. Damit wäre es den Prozeßbeteiligten bei Strafandrohung verwehrt, die geschützten personenbezogenen Daten unbeteiligter Dritter aus den Prozeßakten außerhalb des eigenen Streitverfahrens zu nutzen und an andere zu übermitteln.
   Neben der bereits angesprochenen Pflicht der Gerichte zur Prüfung des Vorlageumfangs nach dem Grundsatz der Verhältnismäßigkeit besteht auch eine Pflicht zur verfassungskonformen Anwendung der in den Prozeßordnungen vorgesehenen Akteneinsichtsrechten der Prozeßbeteiligten und ggf. Dritter. So ist Voraussetzung, daß die Akteneinsicht zur Erreichung des vorgegebenen Zwecks geeignet und erforderlich ist, und daß der mit ihr verbundene Eingriff in die Rechte Dritter nicht außer Verhältnis zur Bedeutung der Sache selbst steht.
   Beispielhaft kann auf einen Beschluß des Hessischen Verwaltungsgerichtshofs vom 7. Oktober 1993 (DÖV 1994, 127) verwiesen werden. Darin hat das Gericht in einem Konkurrentenklageverfahren entschieden, daß der Kläger zwar in die vorgelegten Personalakten eines Mitbewerbers um die Stelle Einsicht nehmen darf, daß aber Grundsätze des Persönlichkeitsschutzes in einem solchen Fall die Erstellung von Abschriften bzw. Vervielfältigungen aus der fremden Personalakte verbieten.

Weitere gerichtliche Schutzmaßnahmen zu Gunsten des Persönlichkeitsrechts unbeteiligter Dritter sind eine dokumentierte Akteneinsicht unter Aufsicht und die Möglichkeit des Vorsitzenden, die Mitnahme von Akten durch einen Rechtsanwalt zu untersagen (vgl. § 100 Abs. 2 Satz 2 VwGO) oder zumindest von der vorherigen Zustimmung des Betroffenen bzw. der personalaktenführenden Stelle abhängig zu machen.

Stichwortverzeichnis *

* Fundstelle zitiert nach Tätigkeitsbericht und Seite