Sächsischer Landtag
1. Wahlperiode

DRUCKSACHE 1/3075

Schutz des Persönlichkeitsrechts im öffentlichen Bereich

1. Tätigkeitsbericht

des

Sächsischen Datenschutzbeauftragten

Dem Sächsischen Landtag

vorgelegt zum 31.März 1993

gemäß §27 des Sächsischen Datenschutzgesetzes

Eingegangen am: 31.3.1993 Ausgegeben am: 6.4.1993

Vorbemerkung zum Sprachgebrauch in diesem Bericht:

Logisch ist zu unterscheiden zwischen biologischem und grammatischem Geschlecht (sexus und genus). Es wäre ein Verlust, diese Unterscheidung aufzugeben; es wäre das Unterfangen, Sprache zu sexualisieren. Ich beteilige mich nicht an solchen Versuchen. Frauen bitte ich, sich auch von scheinbar männlichen, in Wahrheit nur generellen Bezeichnungen gemeint zu wissen: Bauherr, Lehrer, Beamter, Betroffener etc.

Herausgeber: Der Sächsische Datenschutzbeauftragte
Thomas Giesen
Devrientstraße 19
01067 Dresden
(bis 30.6.93: O-8010)
Telefon: 0351 4855909
Fax : 0351 4855993

Postfach 120905
01008 Dresden
(bis 30.6.93: O-8012)

Herstellung: OTTO Verlag und Druckerei

Inhaltsverzeichnis

1 Datenschutz im Freistaat Sachsen

1.1 Datenschutz ist Teil des Schutzes der Persönlichkeit

Breite und Kraft des Schutzes der Individualsphäre vor dem Zugriff des Staates lassen sich nur ermessen, wenn man die Ausgangslage betrachtet. In der DDR gab es keinen Datenschutz. Informationen über Menschen waren die Grundlage ungezügelter Machtausübung staatlicher Organe. Der Bürger wurde als Objekt staatlichen Handelns informationell ausgenutzt; seine Daten wurden zentral verwertet und vor ihm selbst gesichert. Der Mensch wurde von seinem "Datenschatten" begleitet.

Im verfaßten, d. h. sich selbst beschränkenden Rechtsstaat hat sich die Obrigkeit aus unserem Leben so weit wie möglich fernzuhalten. Das gilt für unseren privaten Bereich ebenso wie für Markt und Gesellschaft. Das Persönlichkeitsrecht einerseits und die Anforderungen der Gemeinschaft an den Einzelnen andererseits müssen jedoch zutreffend gewichtet werden. Die sich daraus ergebenden verfassungsrechtlichen Spannungsverhältnisse bedürfen einer menschenfreundlichen und sozialverträglichen, also gerechten Lösung, die auch die neuen Anforderungen in Sachsen erkennt.

1.1.1 Die Würde des Menschen

Der erste Satz des Grundgesetzes (Art. 1 Abs. 1 S. 1 GG) lautet: "Die Würde des Menschen ist unantastbar." Da wird nicht von der "Menschenwürde" gesprochen, sondern von der Würde des Einzelnen. Dieses Bekenntnis zur Individualität ist gleichzeitig die Absage an alle Versuche, mit Hilfe eines philosophischen "Überbaus" die Menschenwürde staatlich abstrakt zu definieren und sodann von Amts wegen zuzuteilen. Der Begriff der Würde des Menschen wird nicht nach allgemeingültigen politischen, juristischen oder staatlichen Vorgaben definiert: Es handelt sich schlicht um Eigenwert und Eigenständigkeit, Wesen und Natur des Menschen schlechthin. Menschen werden in Deutschland nicht mehr in den Dienst einer Idee oder der Gesellschaft gestellt, sie werden nicht "entwickelt" oder umerzogen. Im Grundgesetz setzt sich der Staat bewußt zugunsten des Einzelnen in den Hintergrund, die Gemeinschaft hat keinen höheren Wert und Anspruch als ihre Mitglieder. Deshalb gewährleistet die Gesamtheit der deutschen Rechtsordnung die Uneinschränkbarkeit der Würde des Menschen und seine Selbstverantwortlichkeit.

Als Grund dieser unverlierbaren und unverwechselbaren, höchstpersönlichen Würde des Einzelnen gilt in der stoischen Philosophie und in der Aufklärung die Teilhabe an der Vernunft, nach christlich-jüdischer Auffassung, insbesondere bei den Kirchenlehrern, - und auch nach meinem Verständnis - ist es die Gottebenbildlichkeit des Menschen. Diese Würde gewinnt auch heute Gestalt in der Autonomie jeder Person, in ihrer Möglichkeit, in Freiheit einem Gesetz verpflichtet, also sittlich handeln zu können

Deshalb lautet Art. 2 Abs. 1 GG: "Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."

Die Rechtsordnung, konkretisiert durch die Rechtsprechung des Bundesverfassungsgerichts, sichert die Würde des Einzelnen u. a. in den Bereichen:

- Wahrung menschlicher Identität und Integrität
- Sicherheit des individuellen und sozialen Lebens
- rechtliche Gleichheit der Menschen
- Begrenzung staatlicher Machtausübung
- informationelle Selbstbestimmung (Schutz personenbezogener Daten).

Schon diese Stichworte zeigen, daß Datenschutz keinen Vorrang vor anderen zentralen Vorkehrungen zum Schutz der Würde des Menschen genießt, sondern als Teilbereich des Rechtsstaates in die soziale Ordnung eingebunden ist. Datenschutz darf nicht einseitigen überzogenen Individualismus betonen, sondern hat die Zudringlichkeit des Staates auf ein notwendiges und ausreichendes Maß zu begrenzen. Dem Schlagwort von der "Bürgernähe" der Verwaltung läßt sich entgegenhalten:"...bitte nicht zu nah!"

Die Grenzen des Art. 2 Abs. 1 GG (Schrankentrias), die der persönlichen Freiheit gesetzt sind, gewährleisten ein rechtlich geordnetes und sittliches soziales Leben. Staatliche Ordnungs- und Leistungsfunktionen gewährleisten die Freiheit aller durch ihre Beschränkung.

Die damit entstehenden Ansprüche der Allgemeinheit gegenüber dem Einzelnen wirken jedoch niemals total und auf den Kern seiner Persönlichkeit. Die die rechtliche Ordnung umsetzenden Gewalten haben staunend innezuhalten vor der Individualität und ihrer Würde.
Dies hat konkrete Folgen im alltäglichen Verhältnis der Behörden zu uns allen.

1.1.2 Das Volkszählungs-Urteil

Die Verpflichtung zur Wahrung der Menschenwürde trifft auch Private. Es ist Aufgabe des Gesetzgebers, die Privatrechtsordnung so zu gestalten, daß Würdeverletzungen in der Gesellschaft ausbleiben. Soweit dies durch geschriebene Rechtsregeln nicht erreicht wird, bieten die Grundrechte in ihrer Drittwirkung auf das Zivilrecht die Möglichkeit, Würdeverletzungen im Privatrecht zu sanktionieren. Denn die Freiheitsausübung des einen auf Kosten der Freiheitsmöglichkeiten des anderen wäre unsittlich und mit der "Symmetriebedingung", die das Sittengesetz postuliert, unvereinbar. Wirksamkeit entfaltet das Sittengesetz vornehmlich durch die Generalklauseln der Rechtsordnung (z. B. Verbot der Sittenwidrigkeit, § 138 BGB; Schikaneverbot, § 226 BGB; Treu und Glauben als Maßstab für Verträge, § 242 BGB; Treu und Glauben als Rechtsgrundlage für die Datenerhebung, § 28 Abs. 1 S. 2 Bundesdatenschutzgesetz).

Aus der verfassungsrechtlichen Gewährleistung des "Muttergrundrechts" der freien Entfaltung der Persönlichkeit hat die Rechtsprechung der Zivilgerichte (erstmals Bundesgerichtshof in BGHZ 13, 334, 338) ein allgemeines Persönlichkeitsrecht als absolutes Abwehrrecht entwickelt. Diese Rechtsprechung ist durch das Bundesverfassungsgericht (BVerfGE 34, 269, 281 f.) gebilligt und im Verhältnis der Gemeinschaft zum Einzelnen ausgebaut worden:

Ganz allgemein hatte das Bundesverfassungsgericht schon 1957 bestimmt, daß Gesetze, die zur verfassungsgemäßen Ordnung gehören, die geistige, politische und wirtschaftliche Freiheit nicht so einschränken dürfen, daß die Menschenwürde in ihrem Wesensgehalt angetastet würde. "Hieraus ergibt sich, daß dem einzelnen Bürger eine Sphäre privater Lebensgestaltung verfassungskräftig vorbehalten ist, also ein letzter unantastbarer Bereich menschlicher Freiheit besteht, der der Einwirkung der gesamten öffentlichen Gewalt entzogen ist." (BVerfGE 6, 32, 41)

Konsequenz dieser Rechtsprechung zum Persönlichkeitsrecht war schließlich das "Volkszählungs-Urteil" des Bundesverfassungsgerichts vom 15.12.1983 (BVerfGE 65, 1 ff.): Das informationelle Selbstbestimmungsrecht wurde als Grundrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet und damit "entdeckt". Das Urteil läßt sich in folgenden Kernsätzen zusammenfassen:

- Jeder hat die grundsätzliche Befugnis, selbst darüber zu bestimmen, welche ihn betreffenden Informationen in den öffentlichen Bereich, insbesondere in den Arbeitsbereich der Behörden gelangen. Ausnahmen sind nur erlaubt, wenn dies gesetzlich bestimmt ist;
- unter den Bedingungen der modernen Informationstechnologie gibt es keine "belanglosen" Informationen, sie entwickeln ihre Bedeutung im Verbund;
- alle Phasen der Informationsverarbeitung, also Erhebung, Speicherung, Verwendung und Weitergabe sind vom gesetzlichen Schutz zu erfassen;
- durch organisatorische und verfahrensrechtliche Vorkehrungen ist der Gefährdung des informationellen Selbstbestimmungsrechts rechtzeitig und mit verständlichen und bereichsspezifischen Gesetzen zu begegnen (Normenklarheit);
- jeder muß wissen können, wer was wann und bei welcher Gelegenheit über ihn weiß (Informationstransparenz);
- alle personenbezogenen Daten unterliegen dem Zweckbindungsgrundsatz; jede Zweckentfremdung ist ein erneuter Informationseingriff, der nicht durch Amtshilfe gerechtfertigt ist, sondern einer gesonderten gesetzlichen Grundlage bedarf;
- es gilt der Grundsatz der informationellen Gewaltenteilung: Der gesamte Bereich der öffentlichen Verwaltung ist funktional so zu ordnen, daß nicht einer Behörde gleichzeitig Aufgaben zur Erfüllung übertragen werden, die die Gefahr einer Zweckentfremdung von Daten mit sich bringen, (funktionaler Behördenbegriff);

- wegen der häufig vorhandenen Undurchsichtigkeit der Datennutzung unter den Bedingungen der automatischen Datenverarbeitung und im Interesse eines vorgezogenen Rechtsschutzes ist die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestimmung.[1]

Art. 33 der Sächsischen Verfassung lautet: "Jeder Mensch hat das Recht, über die Erhebung, Verwendung und Weitergabe seiner personenbezogenen Daten selbst zu bestimmen. Sie dürfen ohne freiwillige und ausdrückliche Zustimmung der berechtigten Person nicht erhoben, gespeichert, verwendet oder weitergegeben werden. In dieses Recht darf nur durch Gesetz oder auf Grund eines Gesetzes eingegriffen werden."

Die vorgenannten Grundsätze fordern den Gesetzgeber; sie haben materiell-rechtliche und verfahrensrechtlich-organisatorische Konsequenzen in der gesamten Verwaltung. Hinzu kommt: Datenschutz steht als Grundrecht jedem zu, dem Rechtsbrecher, dem Unsympathischen, dem braven Bürger, dem Ausländer, jedem von uns. Einen "gläsernen Menschen" wünscht die Rechtsordnung nicht, wer immer er auch sein mag.

1.1.3 Kernbereichsgarantie und Verhältnismäßigkeitsgrundsatz

Die Schutzintensität eines Grundrechts ist abgestuft: Mit der Menschenwürde ist ein unantastbarer Kernbereich der Privatsphäre konstituiert. Er kann als die eigentliche Quelle der Freiheit verstanden werden. Denn die Privatsphäre schützt das "So-Sein" des Menschen in seiner Eigenheit und Einzigartigkeit; sie garantiert in ihrem Kern jenen Zustand, in dem der Mensch frei von ungewollten äußeren Einflüssen seine Besonderheit bewahren, weiterentwickeln und regenerieren kann. Dementsprechend betont das Bundesverfassungsgericht, daß ein absoluter Schutz eines "Innenraumes" bestehe, in dem der Einzelne "sich selbst besitzt" und "in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" (BVerfGE 27, 1, 6). Dieser absolut geschützte Persönlichkeitsbereich ist auch nicht schon dann ohne weiteres verlassen, wenn das menschliche Verhalten in den Lebensbereich eines anderen Menschen einwirkt: Auch Sozialbezüge können z. B. im innerfamiliären Bereich absolut schutzwürdig bleiben.

Dieser unantastbare Intimbereich ist die eine Seite, die absoluten Schutz erfordert. Die andere ergibt sich aus der Fülle zusammengeführter Daten und der Tiefe des dadurch möglichen Eingriffs in die Persönlichkeitsstruktur des Einzelnen, z. B. bei einer möglichen Totalüberwachung des Menschen im Sinne der Orwellschen Vision "1984" oder bei der Erstellung von Persönlichkeitsprofilen, wie sie vom Staatssicherheitsdienst tagtäglich erstellt und genutzt wurden. Die Nutzung von Satellitenaufnahmen zur Subventionskontrolle darf nicht den "gläsernen Landwirt" schaffen, die Berechnung

[1] Bei der Diskussion über eine Ergänzung des Grundgesetzes ist zu bedenken, daß es kaum möglich wäre, dies alles in einer Verfassung zu verankern.

von Autobahngebühren nicht zu persönlichen Bewegungsbildern führen. Die Verteidigungslinie, von der der Schutz des Individuums gegenüber dem Anspruch der Allgemeinheit keinen Zoll weichen darf, liegt bei der ungesetzlichen Zusammenführung von Daten.

Die Frage, ob und wieweit menschliches Verhalten und Sein dem unantastbaren Kernbereich oder dem für den Gesetzgeber noch zugänglichen Raum privaten Lebens zugehört, kann befriedigend nur von Fall zu Fall unter Berücksichtigung aller Besonderheiten beantwortet werden (dazu z.B. BVerfGE 34, 238 ff.): Je intensiver der Sozialbezug menschlichen Verhaltens ist, um so eher entstehen die Ansprüche der Allgemeinheit, diesen Sozialbezug in einem gemeinschaftsverträglichen Sinn zu regulieren. "Als gemeinschaftsbezogener und gemeinschaftsgebundener Bürger muß jedermann staatliche Maßnahmen hinnehmen, die im überwiegenden Interesse der Allgemeinheit unter strikter Wahrung des Verhältnismäßigkeitsgebots erfolgen" (BVerfGE 27, 344, 351; seitdem ständige Rechtsprechung). Der Grundsatz der Verhältnismäßigkeit setzt folglich neben der Kernbereichsgarantie dem Gesetzgeber Schranken, ermöglicht aber auch Gestaltungsspielraum. Das Bundesverfassungsgericht wiederholt, daß das Verhältnismäßigkeitsgebot im Bereich des Schutzes der Privatsphäre "strikt" zu wahren sei (aaO., seitdem ständige Rechtsprechung). Mit diesem Postulat ist gemeint, daß für Einschränkungen im Bereich der Privatsphäre besonders gewichtige Gründe erforderlich sind. Denn nur ein solches Verständnis stimmt mit dem "besonders hohen Wert" überein, den das Gericht der Privatsphäre beimißt (BVerfGE 35, 202, 221.). Folglich ist streng zu prüfen, ob und in welcher Tiefe gesetzliche Eingriffe in das Grundrecht zur Erreichung eines gesetzlich definierten öffentlichen Zwecks geeignet, erforderlich, verhältnismäßig und zumutbar sind.

Im Rahmen dieser Abwägung sind vor allem auch kollidierende Grundrechte anderer Menschen zu beachten. Die immer wieder festzustellenden Spannungsverhältnisse zwischen Freiheitsentfaltung des einen und Schutz des anderen (oder den Erfordernissen der Allgemeinheit) sollen möglichst im Wege "praktischer Konkordanz" gelöst werden: Beiden Rechten ist größtmöglicher Entfaltungsspielraum zu sichern. Aber Schiller hat recht: Leicht beieinander wohnen die Gedanken, doch hart im Raume stoßen sich die Sachen. - Das Grundgesetz ist, anders als die (nie eingehaltenen) Verfassungen totalitärer Staaten, ehrlich: Es erweckt nicht den Anschein, es gebe für alles eine in jeder Hinsicht erfreuliche Lösung.

Die vorgenannten Grundsätze binden nicht nur den Gesetzgeber; sie sind auch bei der verfassungskonformen Auslegung unbestimmter Rechtsbegriffe maßgebend.

Verfahrensrechtliche Vorschriften zur Datenerhebung, zur zweckentsprechenden Nutzung und zu ihrer Übermittlung haben ferner die Rechtsschutzgarantie des Art. 19 Abs. 4 GG und die Regeln über ein faires Verfahren (insbesondere zum rechtlichen Gehör, Art. 103 Abs. 1 GG) zu beachten.

1.1.4 Datenschutzgesetz als Auffanggesetz

Das Bundesdatenschutzgesetz schützt den Einzelnen, indem es den Umgang mit personenbezogenen Daten im "nicht-öffentlichen" (besser: "privaten") Bereich sowie durch die Bundesbehörden regelt. Das Sächsische Datenschutzgesetz (SächsDSG) erfüllt diese Aufgabe in allen sächsischen Behörden ("öffentliche Stellen des Freistaates Sachsen, der Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Freistaates Sachsen unterstehenden juristischen Personen des öffentlichen Rechts", § 2 Abs. 1 SächsDSG).

Da das Bundesverfassungsgericht Wert auf inhaltlich hinreichend bestimmte und bereichsspezifische Regelungen zur Ausgestaltung des informationellen Selbstbestimmungsrechts legt, gehen alle spezialrechtlichen Normen, die als besondere Rechtsvorschriften des Freistaates Sachsen oder des Bundes den Schutz personenbezogener Daten regeln, den (allgemeineren) Vorschriften des SächsDSG vor; dieses ist also lediglich Auffang-Gesetz. Normen, die den Sozialbezug des Menschen stärker betonen und damit den generellen Datenschutzstandard des SächsDSG nicht erreichen, befinden sich beispielsweise im Verfassungsschutzgesetz, Polizeigesetz, Stasi-Unterlagengesetz und Archivgesetz; Normen, die den Persönlichkeitsschutz stärker betonen, lassen sich im Sozialrecht, im Gesundheitsrecht, im Melderecht oder im Recht des Umgangs mit Personalakten finden.

In all diesen Fällen hat der Gesetzgeber das Spannungsverhältnis zwischen dem Schutz der Persönlichkeit des Einzelnen und den Ansprüchen der Gemeinschaft nach bisherigen Erkenntnisstand zutreffend und verfassungsgemäß gelöst, verfassungskonforme Auslegung der in den Rechtsvorschriften enthaltenen unbestimmten Rechtsbegriffe dabei vorausgesetzt.

1.1.5 Erforderlichkeit des Umgangs mit Daten und Automaten

Einem häufig vorkommenden Mißverständnis sei vorgebeugt: Unter dem Begriff der Erforderlichkeit können Gesichtspunkte wie "Zeitersparnis", "Verwaltungsvereinfachung", "Bürgernähe", "Personal- und Mitteleinsparung", keinen Platz finden (es sei denn, der Gesetzgeber nennt sie ausdrücklich). Erforderlich ist ein Grundrechtseingriff nur dann, wenn das gesetzlich gesteckte (öffentliche) Ziel auf andere Weise nicht erreicht werden kann und zuvor alle gleichwertigen oder ähnlichen, die Selbstbestimmung weniger belastenden Mittel zur Durchsetzung der öffentlichen Ziele erfolglos ausgeschöpft wurden (condicio sine qua non).

Ich bin mir darüber im klaren, daß Datenschutz manchmal die reibungslose Verwaltungspraxis hemmt und erschwert. Bislang ist es allerdings jeweils gelungen, im Einvernehmen mit den sächsischen Behörden Verfahrensabläufe zu entwickeln, die unsinnigen Aufwand vermieden haben. An aktuellen Beispielen wird belegt, daß Ein-

griffe in das informationelle Selbstbestimmungsrecht häufig nur auf den ersten Blick nötig erscheinen; nähere Beschäftigung mit dem Problem zeigt jeweils, daß der Verzicht auf Inanspruchnahme personenbezogener Daten durchaus möglich ist, *ohne* den öffentlichen Zweck wirklich zu gefährden: Viele Formulare müssen entrümpelt werden, vieles kann einfacher erledigt werden, als sich dies in unseren "Patenländern" (besser: "Partnerländern") eingebürgert hat.

Ich werde weiterhin entschiedenen und grundsätzlichen Widerstand der Idee einiger Technokraten entgegensetzen, die sächsische Verwaltung flächendeckend mit einem Datennetz zu verbinden: Derartige Ideen gelten bei Verwaltungsfachleuten längst als überholt; ich fasse sie als Nachwehen des zentralistischen Sozialismus auf. Ein Transport personenbezogener Daten*massen*, der eine Dauerverbindung rechtfertigen könnte, findet zwischen den Ressorts nicht statt; es wäre ohnehin - von Ausnahmen abgesehen - ein Fehler, wenn die obersten Landesbehörden Einzelfälle entscheiden oder überhaupt zur Kenntnis nehmen würden. Soweit auf der Verwaltungsebene unter Beteiligung mehrerer Stellen entschieden wird, sind "Bündelungsbehörden" im Sinne des Prinzips der Einräumigkeit der Verwaltung, also Landratsämter, kreisfreie Städte und Regierungspräsidien geschaffen worden. Ein landesweites Info-Netz ist zu teuer, wird bald veraltet sein und widerspricht dem datenschutzrechtlichen Zweckbindungsgrundsatz. Es ist naiv zu glauben, Datenmißbrauch könnte technisch verhindert werden: Es geht darum, einen Berg miteinander verwobener codierter Verarbeitungsregeln so zu verwalten, daß z. B. die gewollte Änderung an einer Stelle nicht unbemerkt fehlerhafte Verarbeitungsschritte an einer anderen Stelle hervorruft. Selbst Fachleute räumen ein, da sei es leichter, "einen Sack Flöhe zu hüten."

Vernünftiger Datenschutz versteht sich zugleich als "Entschlackung" behördlicher Datensammlung und als Reduzierung der Verwaltung auf ihre gesetzlichen Kernaufgaben und damit zugleich als Verwaltungsvereinfachung. Informationsnetze der Polizei (im gesetzlich zulässigen Rahmen), Automatisierung des Meldewesens oder der Sozialverwaltung, Vernetzung der Statistik oder Verkehrsleitsysteme - um einige Beispiele zu nennen - werde ich daher unterstützen. Denn praktizierter Datenschutz darf uns nicht in das Zeitalter des Federkiels zurückwerfen.

Wer aber das Heil der Verwaltung in ihrer Automatisierung sucht, irrt sich: Das Werkzeug der Datenverarbeitung hat bisher den Aufwand keineswegs immer verringert. Der hierarchische Aufbau und die rechtsstaatlich gebotene Transparenz behördlichen Handelns werden durch automatisierte Verfahren oft verschleiert. Ständige und kritische Selbstprüfung, ob Datenvorhaltung und -nutzung wirklich notwendig sind, unterbleibt zugunsten des Gedankens "Wenn wir schon einen so leistungsfähigen Rechner haben, dann wollen wir ihn auch nutzen...". Ich sehe die Gefahr, daß in einer von Verkaufsstrategen geförderten Euphorie eine Informationstechnik mit überflüssigen Funktionen, ohne Sensibilität für die Technologiefolgen und ohne streng aufgabenbezogene Dimensionierung, angeschafft wird. Insgesamt befaßt sich die Exekutive übermäßig mit der Datenverarbeitung, ihre Programme engen häufig Initiative und Entscheidungsvielfalt, auch gesunden Drang

zur Vereinfachung und den dringend gebotenen menschlichen Kontakt zum Bürger und seinem besonderen Anliegen, ein.

1.1.6 Datenschutz contra Subsidiaritäts-Prinzip?

Etatismus, also übermäßige Verstaatlichung in einem ganz weiten Sinne, und *Zentralismus*, also übermäßige Zentralisierung, waren prägende Grundzüge des DDR-Systems. Sie haben ganz wesentlich zur Unfreiheitlichkeit und Ineffektivität dieses Systems beigetragen. Dies lag in der Natur der Sache: Etatismus und Zentralismus beeinträchtigen immer Freiheit, Initiative und Effektivität. Den Gegensatz zu Etatismus und Zentralismus formuliert das (allgemeine) *Subsidiaritäts-Prinzip*. Seine schon klassische Definition in der päpstlichen Enzyklika "Quadragesimo anno" 1931 lautet: "Wie dasjenige, was der Einzelmensch aus eigener Initiative und mit seinen eigenen Kräften leisten kann, ihm nicht entzogen und der Gesellschaftstätigkeit zugewiesen werden darf, so verstößt es gegen die Gerechtigkeit, das, was die kleineren und untergeordneten Gemeinwesen leisten und zum guten Ende führen können, für die weitere und übergeordnete Gemeinschaft in Anspruch zu nehmen; zugleich ist es überaus nachteilig und verwirrt die ganze Gesellschaftsordnung".

Das Subsidiaritäts-Prinzip findet sich im Grundgesetz zwar nicht unter den ausdrücklich genannten Organisationsgrundsätzen (Rechtsstaat, Demokratie, Sozialstaat, Bundesstaat). Vor allem die Bundesstaatlichkeit (Art. 20 Abs. 1, 30, 70 Abs. 1 GG) und die Garantie der gemeindlichen Selbstverwaltung (Art. 28 Abs. 2 GG) entsprechen ihm jedoch. Deutsche Rechtstradition, die schlechten Erfahrungen mit dem NS-Regime und mit der zentralistischen DDR lassen das Subsidiaritäts-Prinzip um so attraktiver erscheinen. Ganz allgemein gilt die Erkenntnis: Nachdem der Versuch des Liberalismus, die freie Entfaltung des Individuums als höchstes Gemeinwohlideal anzusehen und den Staat auf bloße Ordnungsfunktionen zu begrenzen, gescheitert ist und der Staat insbesondere wegen seiner Wohlfahrtsaufgaben, als Sozialstaat, eine erweiterte Zuständigkeit für sich in Anspruch nimmt, ist es um so nötiger, eine Aufgabenzuordnung zu finden, welche die Individualität fordert und fördert. Das Subsidiaritäts-Prinzip ergibt sich aus zwei Grundgedanken: Zum einen wird die Verantwortlichkeit und Initiative des Individuums, seiner Familie, seiner örtlichen (oder beruflichen oder sonstigen sozialen) Gemeinschaft - in dieser Reihenfolge der Zuständigkeit - gestärkt, und zum anderen wird *staatliches* Erfüllen gemeinschaftlicher Aufgaben auf das nötige, eben *subsidiäre, Maß* beschränkt, ohne daß damit die Erfüllung der Gemeinschaftsaufgaben beeinträchtigt würde. Im Gegenteil: Dezentralisierung und Deregulierung stärken den Staat, und das, ohne ihn mächtiger zu machen!

Die Anwendung des Subsidiaritätsgrundsatzes dient der Freiheitlichkeit (Entfaltung der Persönlichkeit) und gleichzeitig der Effektivität der Verwaltung. Sie stärkt die Akzeptanz und damit die natürliche Autorität jeder Obrigkeit.

Im Rahmen des ihr offenstehenden Regelungsbereiches gibt die Sächsische Verfassung dem Subsidiaritätsgrundsatz starken Ausdruck. Für die staatliche Verwaltung in Sachsen schreibt Art. 83 Abs. 1 S. 2 vor, daß Aufgaben, die von den nachgeordneten Verwaltungsbehörden zuverlässig und zweckmäßig erfüllt werden können, *diesen* zuzuweisen sind. Außerdem wird in der Sächsischen Verfassung auf die gemeindliche Selbstverwaltung und die Übertragung staatlicher Aufgaben auf die Gemeinden besonderer Wert gelegt, wie die ausführliche Regelung in den Artikeln 84 - 90 zeigt. Das bedeutet insbesondere: Wenn den Gemeinden staatliche Aufgaben zur Erfüllung übertragen werden, behalten sie ihre Personal-, Organisations-, Planungs- und Finanzhoheit. Konkret im Hinblick auf den Einsatz automatischer Datenverarbeitung heißt das: Die technische Entwicklung zu leistungsfähigeren PC-Anlagen und die Möglichkeit, diese örtlich zu vernetzen, ermöglicht selbstbewußten Gemeinden und ihren Verbänden - aber auch privaten Unternehmen, die im Auftrag der öffentlichen Hand arbeiten -, eine eigene leistungsfähige Datenverarbeitung aufzubauen, die von Zentralrechnern und landeseinheitlichen Informationssystemen unabhängig ist.

Manche meinen, die Dezentralisierung der staatlichen Aufgabenerfüllung und das Subsidiaritäts-Prinzip insgesamt gerate in einen Gegensatz zum Schutz des Persönlichkeitsrechts. Die informationelle Selbstbestimmung sei besser in großen Zentralrechnern zu gewährleisten. Dies halte ich für einen fundamentalen Irrtum und eine falsches Verständnis des Volkszählungsurteils. Dort wird nämlich gerade die Massendaten-Verarbeitung als Gefahr erkannt: Je weiter von mir entfernt meine Daten gesammelt werden, um so unüberschaubarer ist ihre Verwendung, und desto geringer wird meine Kraft, ihrer Zweckentfremdung entgegenzutreten.

Je kleiner und näher die Gemeinschaft ist, in der ich lebe, um so eher kenne ich den Wissensstand meiner sozialen Umwelt über mich und um so leichter kann ich ihn beeinflussen und mich an ihm orientieren. Darauf aber kommt es an: "Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, in eigener Selbstbestimmung zu planen oder zu entscheiden" (BVerfGE 65, 1, 42).

Das bedeutet insbesondere:
Die gewachsenen Strukturen der Lebenswirklichkeit, die sich in den neuen Bundesländern wiederbeleben, dürfen durch Datenschutz nicht abgetötet werden.
Die Forderung nach einer anonymen Massengesellschaft, in der die Daten der Bürger spezialisiert verwendet und in sektoraler Zuständigkeit, fern vom Einzelnen und zentralistisch verwaltet werden, mag das Idealbild eines "Datenschützers mit Ofenrohrblick" sein; das Bundesverfassungsgericht hingegen sieht die Gefahren für das

Persönlichkeitsrecht, also die Würde des Einzelnen, jedoch nicht schlechthin darin, daß z. B. der Bürgermeister eines Dorfes viel, wenn nicht "alles" über seine Einwohner weiß, sondern führt aus, daß die Befugnis des Einzelnen, selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, "unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes" bedarf (BVerfGE 65, 1, 42). "Diese Befugnis ... ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muß, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus - vor allem beim Aufbau integrierter Informationssysteme - mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann" (BVerfGE 65, 1, 42).

1.1.7 Der Sächsische Datenschutzbeauftragte

Art. 57 der Sächsischen Verfassung ordnet den Sächsischen Datenschutzbeauftragten unter zwei Gesichtspunkten in das System der Institutionen des Freistaates ein: Zunächst unter demjenigen des *Rechtsstaates,* nämlich "*zur Wahrung des Rechtes auf Datenschutz*". Der Datenschutzbeauftragte hat der neuartigen durch die EDV sichtbar gewordenen besonderen Gefährdung des Grundrechts auf informationelle Selbstbestimmung für jeden Einzelnen vorzubeugen, Verständnis für eine Änderung des Verwaltungshandelns zu wecken und vor den Gefahren der Informationstechnik zu warnen.

Der andere Gesichtspunkt, unter dem die Sächsische Verfassung den Datenschutzbeauftragten sieht, ist derjenige der *Demokratie.* Art. 57 der Sächsischen Verfassung nennt als weiteren Zweck der Einrichtung des Datenschutzbeauftragten nämlich die "*Unterstützung bei der Ausübung der parlamentarischen Kontrolle*" und ordnet den Datenschutzbeauftragten dem Landtag zu. Dieses Staatsorgan vertritt das Volk (repräsentative Demokratie), von dem alle Staatsgewalt ausgeht (Art. 20 Abs. 2 S. 1 GG). Es bindet Regierung und Verwaltung an seine Gesetze und kontrolliert sie. Durch Kleine und Große Anfragen, Untersuchungsausschüsse sowie durch Ausübung des Zitierungs- und des Haushaltsrechtes, und - allerdings nur beratend und unterstützend - durch den Datenschutzbeauftragten.

Dieser ist in der Ausübung seines Amtes unabhängig, weisungsfrei und nur dem Gesetz unterworfen (§ 23 Abs. 4 S. 1 SächsDSG).

Der Datenschutzbeauftragte "bezahlt" seine Unabhängigkeit (Ministerialfreiheit) damit, daß ihm keine Exekutivbefugnisse zustehen, er also lediglich raten, jedoch nicht befehlen kann. Als schärfste Sanktion steht ihm ein - exekutivrechtlich streng genommen folgenloses - Beanstandungsrecht zu, das jedoch regierungsinterne, parlamentarische und über die Medien auch politische Wirkungen entfalten kann. Politisches Kalkül jedoch steht dem Datenschutzbeauftragten in seiner unabhängigen und dem Recht dienenden Funktion nie zu.

Bei seinem Rat und seinen Überprüfungen ist der Datenschutzbeauftragte nicht darauf beschränkt, den Umgang der Exekutive mit personenbezogenen Daten an den Vorschriften des Sächsischen Datenschutzgesetzes zu messen; dieses schreibt vielmehr vor, daß er vorrangig zu prüfen hat, ob der Gebrauch der personenbezogenen Informationen zur gesetzlichen Aufgabenerfüllung einer Behörde gehört, in spezialgesetzlichen Normen geregelt ist und den oben genannten Verfassungsgrundsätzen entspricht.

1.1.8 Datenschutz mit Maß

Kein Zweifel: "Der Datenschutz" ist in den Verwaltungen unbeliebt. Nicht zu unrecht ist er in Verruf geraten, sich zum Selbstzweck zu entwickeln und das Rumpelstilzchen-Prinzip ("Ach wie gut, daß niemand weiß...") über alles zu stellen. Der Datenschutzbeauftragte wird angesehen als ein ewiger Nörgler, der vernünftige, zweckdienliche Verwaltungsentscheidungen erschwert oder gar verhindert. Das mag auch daran liegen, daß die gewachsene und eingefahrene Verwaltungspraxis - verfassungsgerichtlich erst seit Ende 1983 verbindlich - mit einer jungen Erkenntnis konfrontiert wurde, die fast das gesamte Verwaltungshandeln verändert, und zwar im materiell-rechtlichen, aber auch im organisatorisch-verfahrensrechtlichen Bereich. Die damit verbundene "Störung" wird dann verdächtigt, den Sinn der Verwaltung insgesamt in Frage zu stellen. In Wahrheit müßte sie erfrischend und selbstkritisch wirken. Deshalb gilt es, ein vernünftiges (datenschutzrechtlich reduziertes) Maß zu finden. Wie der Staat gewinnt auch der Datenschutz durch kluge Selbstbeschränkung an Autorität. In den jungen Bundesländern hat man einen Vorteil: Beim Aufbau einer neuen Verwaltung lassen sich alte Fehler allerseits vermeiden. Und es fehlt auch nicht an einem darauf gerichteten Streben:
Ich habe in Sachsen, wohl bedingt durch das oft hautnahe Erleben des total-informierten Staates, ein erfreuliches Interesse an Datenschutzfragen erlebt. Das Bürgerrecht auf eine "gläserne Verwaltung" wird hier nachdrücklich gefordert; den "gläsernen Menschen" des real-existierenden Sozialismus wird es in Sachsen nicht mehr geben. Es gelingt der Verwaltung auch nicht, den Datenschutz bei der eigensüchtigen Verfolgung von Geheimhaltungsinteressen zum Vorwand zu nehmen.

Neben dem Grundrecht auf informationelle Selbstbestimmung gibt es weitere, ebenso wichtige Grundrechte, deren Schutz die Exekutive zu gewährleisten hat. Von ihr wird verlangt, daß sie gesellschaftliche Veränderungen, Gefährdungen und neuen Situationen unverzüglich gerecht wird und dabei Sicherheit und Wohlstand garantiert. Als Beispiel sei der Ruf nach der Zulässigkeit heimlicher Gesprächs- oder Bildaufzeichnungen in Wohnungen ("Großer Lauschangriff") gegen Verdächtige der "organisierten Kriminalität" genannt. Der Datenschutz betont demgegenüber auftragsgemäß verfassungskonforme Strukturen und bildet ein beharrliches und beharrendes Korrektiv gegen - politisch oft kurzlebige - Aktionismen; dies schon deshalb, weil nur gesetzliche Grundlagen den Eingriff in ein Grundrecht ermöglichen. Eine datenschutzrechtliche Neubewertung ist dennoch nötig: Der Lauschangriff sollte in einem neuen Bundesgesetz nur im Kernbereich der Wohnung untersagt bleiben. (In Sachsen gibt es heute allerdings dringendere Probleme, in erster Linie beim Neuaufbau einer privaten Wirtschaftsstruktur).

Insbesondere unter den Bedingungen einer gewaltigen Umorganisations- und Aufbauarbeit im Freistaat Sachsen muß sich der Datenschutzbeauftragte beschränken und nicht übertrieben agieren. Ich berate gerne; Fehler nehme ich nicht übel, wenn sie eingesehen werden. Beanstandungen spreche ich selten und nur dann aus, wenn meine Hinweise auf Ignoranz stoßen. Bis ein Stamm sächsischer Verwaltungsfachleute entstanden ist, wird es natürliche Schwierigkeiten geben, die ich berücksichtige. - Dies alles gilt auch für mich selbst: Ich bitte dafür schon jetzt um Verständnis.

Die neue Situation im Freistaat Sachsen bietet eine (unwiederbringliche) Gelegenheit, eine möglichst wenig etatistische, sondern auf Individualismus und Initiative des Einzelnen setzende, also zurückhaltende und deshalb geachtete Verwaltung einzurichten. Wenn der Datenschutzbeauftragte daran mitwirkt und, Augenmaß bewahrt, wird er ernst genommen, nur dann wird er gehört und erfüllt er seinen gesetzlichen Auftrag.

Darum bemühe ich mich.

1.2. Aufbau einer Dienststelle, Entstehung und Besonderheiten des Sächsischen Datenschutzgesetzes

Nach dem Einigungsvertrag (Anl. I Kapitel II Sachgebiet C Abschnitt III Nr. 3) fanden die Bestimmungen des Bundesdatenschutzgesetzes zur Durchführung des Datenschutzes in der Verwaltung im Beitrittsgebiet Anwendung. Der Bundesbeauftragte für den Datenschutz übte die Kontrolle als Organ des Freistaates Sachsen aus »bis zur Schaffung einer Datenschutzkontrolle,, längstens jedoch bis zum 31. Dezember 1991<<.

Im April 1991 erhielt ich von Ministerpräsident Prof. Dr. Kurt Biedenkopf im Einvernehmen mit dem Präsidenten des Sächsischen Landtages, Erich Iltgen, den Auftrag, den Arbeitsstab des Landesbeauftragten für den Datenschutz zu leiten. Der Arbeitsstab hatte insbesondere die Aufgabe, die Erarbeitung eines Sächsischen Datenschutzgesetzes zu begleiten. Beim Staatsministerium des Innern war bereits ein Referat als Aufsichtsbehörde für den Datenschutz bei der Datenverarbeitung nichtöffentlicher Stellen eingerichtet worden.

Meine der Staatskanzlei zugeordnete Dienststelle bestand zunächst aus meiner Sekretärin und mir. Ich habe in erster Linie in Bonn, Mainz und Wiesbaden die für einen »professionellen Datenschützer« erforderlichen Kenntnisse gesammelt. Bei diesen Informationsbesuchen waren mir der Bundesbeauftragte für den Datenschutz und die Landesbeauftragten für den Datenschutz von Rheinland-Pfalz und Hessen sehr behilflich. Sie leisteten in kollegialer Weise jede erbetene Hilfe. So kam dann auch im September 1991 der erste wertvolle fachliche Beistand, ein »Leihbeamter« vom Bundesbeauftragten für den Datenschutz, der für den Aufbau der neuen Dienststelle zur Verfügung stand. Ihm schloß sich im Oktober ein Verwaltungsjurist, Ruhestandsbeamter aus Baden-Württemberg, an.

In der Zwischenzeit waren die Verhandlungen über den Entwurf eines Sächsischen Datenschutzgesetzes voll angelaufen, nachdem im September eine Anhörung des Bundesbeauftragten für den Datenschutz und der Landesbeauftragten für den Datenschutz von Baden-Württemberg und Hessen stattgefunden hatte. In der Sitzung des Innenausschusses des Sächsischen Landtages am 18. Oktober 1991 in Hoyerswerda wurde über einen Gesetzentwurf der CDU-Fraktion (Drucksache 1/523) sowie über Änderungsanträge der CDU-Fraktion und der Fraktionen der SPD und des Bündnis 90/Grüne verhandelt. Da zunächst keine Einigung zu erzielen war, beschloß der Innenausschuß auf Vorschlag seines Vorsitzenden, Abg. Hartmut Ulbricht, Anfang November zwei Klausurtagungen durchzuführen, denen sodann die abschließende Behandlung im Innenausschuß folgen sollte. Die Tagungen fanden als interfraktionelle Gesprächsrunden statt. Anwesend waren außer den von den Fraktionen benannten Abgeordneten und zwei Fachleuten der Staatsregierung nichtparlamentarische Sachverständige; auch ich war zugezogen worden. Die Verhandlungen zeichneten sich durch das große Bemühen aller Beteiligten aus, trotz oder gerade wegen der Kornpliziertheit der Materie eine Einigung zu erzielen, die nach Möglichkeit allen Ansprüchen gerecht wird. Ich sehe eine derartige Gesprächsrunde auch im nachhinein als ein Vorbild dafür an, wie in einem demokratischen Staat trotz gegensätzlicher politischer Meinung gemeinsame Grundanliegen in kürzester Zeit erfüllt werden können. Die hervorragende Vorarbeit - es wurden weit über 100 Änderungen konsensfähig vorformuliert - trug dann auch reiche Früchte. In der Sondersitzung des Innenausschusses am 7. November konnte man schon in die endgültige Beschlußfassung zum Datenschutzgesetz eintreten. Es wurde paragraphenweise abgestimmt. Die Schlußabstimmung ergab eine Zustimmung zu der Drucksache 1/523 und den dazu beschlossenen Änderungen mit 14:0:2 Stimmen.

Schon am 21. November 1991 konnte der Landtag in die 2. Lesung des Gestzes zum Schutz der informationellen Selbstbestimmung (Sächsisches Datenschutzgesetz) eintreten.

Das Gesetz wurde, nachdem zuvor über weitere kleinere Änderungsanträge abstimmt worden war, vorn Sächsischen Landtag bei einigen Stimmenthaltungen und bei zwei Gegenstimmen beschlossen.

Der Abgeordnete Martin Rade, F.D.P., hatte zuvor ausgeführt, »der Brückenbau- trotz eines vorherigen Crashs« - sei »über ein fünfköpfiges Redaktionskollegium erfolgt, das aus den Gesetzentwürfen Konsens und Dissens zusammenformiert und offene Punkte herauskristallisiert« habe, Das sei ein Weg, der auch in Zukunft beschritten werden sollte.

Vor der Schlußabstimmung hatte schon der Staatsminister des Innern, Herr Eggert, darauf hingewiesen, daß das Gesetz auf einem außerordentlich hohen Niveau angesiedelt sei. Dieses hohe Niveau sei nicht zuletzt dem Umstand zu verdanken, daß das Gesetzeswerk das Ergebnis einer langen und gründlichen Diskussion zwischen allenFraktionen sei und der Entwurf auf weitestgehendem Konsens beruhe

Das unter dem 11. Dezember 1991 erlassene Sächsische Datenschutzgesetz am 13. Dezember 1991 im Gesetzblatt verkündet und trat am Tage darauf in Kraft (GVBI. Nr. 32/1991 S. 401). Es ist aus meiner Sicht ein modernes Werk mit einem hohen Standard. Damit konnte auch der Sächsische Datenschutzbeauftragte gewählt werden. Er ist vom Landtag mit der Mehrheit seiner Mitglieder auf sechs Jahre zu wählen. Ich war von der Fraktion der CDU zur Wahl vorgeschlagen worden. Die Wahl fand am 20. Dezember 1991 in geheimer Abstimmung statt; bei 137 gültigen Stimmen stimmten 98 Abgeordnete mit Ja, 23 mit Nein, 16 enthielten sich der Stimme. Anschließend wurde mir vom Präsidenten des Sächsischen Herrn Erich Iltgen, dessen Dienstaufsicht ich unterstehe, die Ernennungsurkunde ausgehändigt.

Der Sächsische Datenschutzbeauftragte wird beim Sächsischen Landtag berufen. Dementsprechend befindet sich der Sitz im Bereich der Landtagsverwaltung.

Für die Erfüllung seiner Aufgaben ist dem Datenschutzbeauftragten die notwendige Personal und Sachausstattung zur Verfügung zu stellen. Ich bin dankbar, daß der Landtagspräsident dem Datenschutz großes Verständnis entgegenbringt. Organisatorisch wurde und werde ich von den Damen und Herren der Landtagsverwaltung dankenskenswerterweise uneingeschränkt unterstützt. Mit der Personalausstattung kann ich sehr zufrieden sein. Nach dem Haushalt 1993 sind einschließlich des Datenschutzbeauftragten für die Dienststelle 19 Stellen ausgebracht, davon 13 Stellen des höheren Dienstes. Nicht nur fachlich, wobei allerdings der Aufgabe entsprechend die Juristen überwiegen, sondern auch nach dem landsmannschaftlichen Herkommen sind wir ein heterogenes Team. Es ist erfreulich zu wissen und zu erfahren, daß sich nur die Individuen unterscheiden. Die realisierte

deutsche Einheit zeigt sich uneingeschränkt positiv auch in unserer Dienststelle.

Auf die nähere inhaltliche Darstellung des Sächsischen Datenschutzgesetzes habe ich bewußt verzichtet. Sie soll ausführlich an anderer Stelle erfolgen. Trotzdem weise ich nachfolgend auf einige Besonderheiten des Gesetzes hin:

Der Begriff der Datenverarbeitung umfaßt gemäß § 3 Abs. 2 SächsDSG als Oberbegriff -anders als das Bundesdatenschutzgesetz, das Erheben, Verarbeiten, Sperren und Löschen kennt - alle Formen des Umgangs mit personenbezogenen Daten (Erheben, Speichern, Verändern, Übermitteln, Nutzen, Sperren, Löschen). Mithin erfaßt die »Verarbeitung« jeglichen Umgang mit Daten. Sie hat daher immer auch zu fragen: Woher stammen meine Informationen, wie wurden sie erhoben, wohin gelangen sie? Die Terminologie entspricht so einem umfassenden Grundrechtsschutz.

Bewußt verzichtet das Gesetz auf die Institution des behördlichen Datenschutzbeauftragten. Damit betont es die ungeteilte Verantwortung des Dienststellenleiters für den Umgang mit personenbezogenen Informationen. Ein behördlicher Datenschutzbeauftragter kann damit weder Feigenblatt noch Sündenbock werden. Die Organisationshoheit der Minister, Landräte, Bürgermeister und Universitätsrektoren bleibt unangetastet (siehe 16.1.2).

Ferner verzichtet das Gesetz darauf, daß beim Sächsischen Datenschutzbeauftragten ein zentrales Dateiregister geführt wird. Der damit verbundene bürokratische Aufwand schiene mir unverhältnismäßig; ich kann jederzeit - auch auf Bitten von Petenten - die internen Dateiregister nach § 10 SächsDSG abrufen, kontrollieren und Betroffenen Einsicht gewähren (§ 28 SächsDSG), damit sie ihr Auskunftsrecht »vorbereiten« können.

Die konsequente Altdatenregelung in § 35 des Gesetzes dient - wie ich finde - in vorbildhafter Weise einer geordneten und fairen Kenntnis der Vergangenheit. Sie wird soweit ich sehe - von allen maßgeblichen politischen Gruppen getragen. Denn nur die Wahrheit wird uns frei machen.

1.3 Altdaten

1.3.1 Ausgangslage

Nach der Wiedervereinigung stellte sich die Situation hinsichtlich der sog. Altdaten im Beitrittsgebiet wie folgt dar:

- Umfang und Inhalte personenbezogener Datenbestände der DDR waren nur grob bekannt.
- Unbekannt war insbesondere, was mit den Datenbeständen geschehen war, in denen sich die Unterdrückungsmaßnahmen des Unrechtsstaats DDR in Bezug auf

einzelne Personen niedergeschlagen haben (Ausnahme Stasi-Akten).
- Zur Aufrechterhaltung der Verwaltung mußten die zu DDR-Zeiten erhobenen Daten im allgemeinen weiter genutzt werden, auch wenn sie Bestandteile enthielten, deren Erhebung bzw. Verarbeitung nach jetzigen Recht unzulässig wäre.
- Personenbezogene Daten waren in Form von Dateien und Akten »überall« in der DDR entstanden, d. h nicht nur im »eigentlichen« öffentlichen Bereich, sondern z. B. auch in Wirtschaftseinrichtungen und gesellschaftlichen Organisationen.

Es wäre vordringlich gewesen, zunächst diese Datenbestände zu sichern, d. h. ihre Vernichtung oder Entwendung sowie eine unbefugte Verwendung ihres Inhaltes zu verhindern. Eine Regelung, die für eine solche Sicherung sorgen soll, brachte leider erst das am 14. Dezember 1991 in Kraft getretene Sächsische Datenschutzgesetz (SächsDSG), das die im Einigungsvertrag (Anlage 1 Kapitel H Sachgebiet C Abschnitt III Nr. 3) getroffene Übergangsregelung ablöste.

§ 35 SächsDSG verpflichtet jeden Besitzer von Altdatenbeständen, insbesondere von alten Akten, dem Sächsischen Datenschutzbeauftragten bis zum 31. März 1992 ein Verzeichnis dieser Bestände zuzuleiten (Abs. 2 Satz 1), diese unter Verschluß zu nehmen (Abs. 2 Satz 2) und sie auf Verlangen dem Sächsischen Staatsministerium des Innern oder einer von diesem genannten Behörde vorzulegen bzw. zu übergeben (Abs. 4). Außerdem verpflichtet die Vorschrift jedermann, nach besten Wissen von sich aus Angaben über nicht mehr vorhandene Altdatenbestände zu machen (Abs. 3).

Es ist also folgende Aufgabenteilung vorgenommen worden: Der Sächsische Datenschutzbeauftragte verschafft sich einen Überblick über Ort, Gegenstand, Umfang und Art der Datenbestände unter besonderer Berücksichtigung der Belange Betroffener. Das Staatsministerium des Innern entscheidet auf dieser Grundlage, welche Daten archiviert oder vernichtet werden sollen oder welche weiterverwendet werden dürfen.

1.3.2 Maßnahmen, Erfahrungen

Die in § 35 SächsDSG begründete Meldepflicht gegenüber dem Sächsischen Datenschutzbeauftragten wurde von mir durch die Bekanntmachung vom 20. Februar 1992 (SächsABI. S. 211) konkretisiert (vgl. Nr. 16. 1. 1) Dabei ist insbesondere klargestellt worden, daß - dem Schutzzweck der Regelung entsprechend - dem Tatbestandsmerkmal *»für Zwecke der öffentlichen Verwaltung«* in § 35 Abs. 1 SächsDSG die weite Auffassung des DDR-Systems von »Partei und Staat« zugrundegelegt worden ist. Öffentliche Verwaltung in diesem Sinne ist, was mit den Datenbeständen geschehen war, in fentliche Verwaltung *in diesem Sinne ist bzw. war jede Tätigkeit, die auf Machtausübung seitens politischer oder staatlicher Organe der DDR beruhte und die zur Folge hatte, daß das Individuum in ein Abhängigkeitsverhältnis gegenüber der tätigwerdenden Organisation gebracht worden ist*

Der Bekanntmachung war ein Meldevordruck beigefügt. Seitdem sind bei mir bis heute Meldungen eingegangen, die 35 Aktenordner füllen. Der weitaus größte Anteil davon stammt von Schulämtern und Schulen (13 Ordner) sowie aus dem engeren Bereich der öffentlichen Verwaltung: Von Ministerien, Regierungspräsidien, kreisfreien Städten, Landkreisen und Gemeinden (15 Ordner). Gering war der Rücklauf von privatisierten bzw. von der Treuhandanstalt verwalteten Wirtschaftsunternehmen (4 Ordner). Nur ca. 90 Unternehmen haben geantwortet, eigentliche Verzeichnisse haben davon wiederum nur ca. 60 geliefert. Die übrigen teilten mit, daß keine Altdatenbestände vorhanden bzw. daß diese bereits vernichtet, anderen Unternehmensbereichen überlassen oder als politisch relevante Altdatenbestände (z. B. SED-Unterlagen) den entsprechenden (Parteileitungs-) Gremien übergeben worden seien. Die restlichen Verzeichnisse stammen von ehemaligen gesellschaftlichen Organisationen und Parteien sowie Kirchen und Archiven.

Bis jetzt konnten erst die Verzeichnisse von Wirtschaftsunternehmen und Schulen ausgewertet werden. Deren qualitative Aussage reicht vom bloßen Schlagwort als Bezeichnung des jeweiligen Altdatenbestandes, z. B. »Schriftverkehr mit gesellschaftlichen Organisationen«, bis zu höchst detaillierten Auflistungen. Rückschlüsse auf den tatsächlichen Informationsgehalt des Altdatenbestandes sind oft nur sehr beschränkt möglich. Um mir ein besseres Bild zu verschaffen, habe ich deshalb einige Wirtschaftsunternehmen und eine Fachschule aufgesucht, um an Ort und Stelle bestimmte Datenbestände in Form von Altakten anhand der vorgelegten Verzeichnisse zu überprüfen. Ausgewählt worden waren diese Stellen wegen der begründeten Vermutung, daß sich dort Altdatenbestände mit starkem Persönlichkeitsbezug bzw. politischer Brisanz befinden könnten. Im übrigen wurde auch der Sicherungsgrad (§ 35 Abs. 2 Satz 2 SächsDSG) geprüft. Die Bestände waren ausreichend gesichert, entweder in besonderen »Betriebsarchiven« oder unter unmittelbarer Kontrolle der Geschäftsleitung bzw. des betrieblichen Datenschutzbeauftragten. Allerdings ist die räumliche Unterbringung im allgemeinen unbefriedigend, und es war von daher verständlich, daß eine baldige Entlastung mindestens von Teilbeständen der unter Verschluß zu haltenden Altdaten seitens der Unternehmen gefordert wurde.

Anläßlich der Klärung des Verbleibs von personenbezogenen Datenbeständen liquidierter Wirtschaftsunternehmen konnte im Dresdener Archiv der Treuhandanstalt, dem sog. »Sachsendepot«, festgestellt werden, daß dort die entsprechenden Bestände des Treuhandbereiches Dresden ordnungsgemäß eingelagert werden und zuverlässig gesichert sind. Bei persönlichen Vorsprachen Betroffener, insbesondere zu Rentenfragen, wird Auskunft erteilt oder auch Einsicht in die der jeweiligen Person eindeutig zugeordneten Personal- oder Lohn/Gehalts-Unterlagen genommen, wobei Datenschutzbelange vorbildlich gewahrt werden.

Die gemeldeten Altdatenbestände schulischer Einrichtungen brachten keine neuen Erkenntnisse. Erwartungsgemäß ähneln sich die Meldungen der Schulen sehr,

begründet durch den extrem restriktiven Charakter des DDR-Volksbildungsregimes. Hier st bei der Stichprobe in einem Fall - an einer Fachschule - personenbezogenes Aktenmaterial festgestellt worden, das einen Vorgang mit erheblicher, politisch motivierter Verletzung des Persönlichkeitsrechts zum Inhalt hat. Allgemein ergaben die Verzeichnisanalysen und die Besuche folgende Erkenntnisse
Es gibt einen sehr großen Bestand noch unerschlossener Altakten mit inhaltlichen Bezugnahrnen auf »gesellschaftliche Organisationen«, wobei es sich jedoch im allgemeinen um Protokolle, Lageberichte etc. handelt, die pedantisch und weitschweifig, aber doch recht belanglos sind. Gerade umfangreiche Akten enthalten im allgemeinen – wenn überhaupt - oft nur weit verstreut Daten mit starkem Persönlichkeitsbezug. Brisante »Hintergrundakten« sind nach einhelliger Meinung der betrieblichen Datenschutzbeauftragten nicht (mehr) vorhanden. Daß Aktenbestände für Auskünfte für Wiedergutmachungsansprüche benötigt und genutzt werden können, wird als unwahrscheinlich eingeschätzt. Nur in *einem* Unternehmen wurde bemerkenswertes SED-Akteninaterial aufgefunden, das offenbar aus Versehen nicht »rechtzeitig« entfernt bzw. vernichtet worden war.

Personalakten müssen dagegen zur Klärung sozialversicherungsrechtlicher Fragen häufig herangezogen werden.

1.3.3 Große Anfrage der CDU-Fraktion des Sächsischen Landtages

Am 16. September 1992 richtete die CDU-Fraktion des Sächsischen Landtags eine Große Anfrage an die Staatsregierung zum Thema »Sicherung von Akten über Korruption und Amtsmißbrauch« (Drucksache 1/2360), welche die politische Bedeutung der Altdatenproblematik hervorhob. In die Beantwortung durch den Staatsminister des Innern vom 7. Dezember 1992 sind meine bis zu diesem Zeitpunkt erreichten zu Arbeitsergebnisse eingeflossen.

Als wesentliche Punkte dieser Antwort seien genannt:

- Rechtsgrundlage für die Aufbewahrung der Altdatenbestände in staatlichen Archiven ist bis zur Verabschiedung des Sächsischen Archivgesetzes die Verordnung über das Staatliche Archivwesen der DDR vom 11. 3. 1976 (GBI. der DDR Teil 1 Nr. 10 S. 165), ergänzt durch Bestimmungen des Bundesarchivgesetzes vom 6. 1. 1988 (BGBl. 1 S. 62), zuletzt geändert am 13. 3. 1992 (BGBl. 1 Für den S. 506). Nichtstaatliche Archivträger, z. B. Kommunen, lehnen sich an diese Regelungen an.

- Bereits vor Inkraftreten der Altdatenregelung gemäß § 35 SächsDSG ist durch Archive umfangreiches Schriftgut aus staatlichen, kommunalen und sonstigen Beständen übernommen worden. Bedeutsame Unterlagen sind die Bestände der Landesregierung Sachsen 1945-52, der Räte der Bezirke 1952-90, der SEDLandes- bzw. -Bezirksleitungen, der Räte der Kreise und Städte, insbesondere der Abteilungen Inneres und Staatliches Eigentum/Finanzen; außerdem Akten gerichtlicher und staatsanwaltschaftlicher Art, der Polizeibehörden und des StrafVollzugs.
- Eine Löschung oder Vernichtung von Altdatenbeständen ist durch die Staatsregierung bisher in keinem Fall verfügt worden.
- Eine künftige Archivierung sollte nach dem Provenienzprinzip, d. h. geordnet nach der Herkunft der Akten, erfolgen.
- Zur Akteneinsicht durch Betroffene erscheint eine gesonderte archivgesetzliche Regelung erforderlich (welche Personen genießen Schutz vor Preisgabe ihrer Identität und welche nicht?).
- Die Altdatenbestände von CDU und FDP sind den zentralen Archiven der jeweiligen Parteistiftungen übergeben worden, die der SED-Bezirksarchive wurden in die entsprechenden Staatsarchive übernommen, desgleichen Unterlagen aus Bezirksarchiven und von Bezirksleitungen (Leipzig, Dresden) ehemaliger gesellschaftlicher Organisationen (Freier Deutscher Gewerkschaftsbund, Freie Deutsche Jugend, Arbeiter- und Bauerninspektion, Kulturbund, Vereinigung der gegenseitigen Bauernhilfe).

Die Staatsregierung hat im Dezember 1992 den Entwurf eines Archivgesetzes in den Landtag eingebracht, bei dessen parlamentarischer Beratung auch die Frage des Einsichtsrechts Betroffener erörtert werden wird (vgl. unter 5.8).

1.3.4 Künftige Maßnahmen

Der Vollständigkeitsgrad der mir gemäß § 35 SächsDSG zugegangenen Meldungen ist, was den im engeren Sinn öffentlichen Bereich betrifft, zufriedenstellend. Ich plane weitere Kontrollbesuche, um eine klare Grundlage für Empfehlungen für künftige Entscheidungen des Staatsministeriums des Innern über den Verbleib der Bestände zu gewinnen.

Wegen des bisher unbefriedigenden Rücklaufes aus dem Unternehmensbereich werde ich die Betriebe mit einer bestimmten Mindestbeschäftigtenanzahl auf der Grundlage von Unternehmensverzeichnissen der Treuhandanstalt schriftlich nochmals an 3 (GBI. der ihre Meldepflicht erinnern, um auch hier möglichst lückenlos die Altdatenbestände zu sichern.

Für den Komplex der schulische Altdaten wird demnächst eine von mir angeregte gemeinsame Verwaltungsvorschrift der Staatsministerien für Kultus und des Innern erlassen werden, wonach Schulen ihre Bestände nicht mehr gemäß § 35 Abs. 2 Satz 2

SächsDSG unter Verschluß halten müssen. Hiervon ausgenommen bleiben durch Einzelerlaß besonders bezeichnete Altunterlagen, denen zeitgeschichtliche Bedeutung zukommt oder die der Rehabilitierung oder dem Auskunftsanspruch einzelner dienen können. Für andere Altdatenkomplexe sollen entsprechende Zwischenregelungen getroffen werden. Langfristig wird durch Einzelerlaß zu entscheiden sein, welche Bestände an die staatlichen Archive abzugeben sind.

Die Aufarbeitung der gesamten Altdatenproblematik wird nicht vor Ende 1993 beendetdet sein.

1.4 Weitere Nutzung des ZER-Meldedatenbestandes?

Nach dem 31. Dezember 1992 ist gemäß Einigungsvertrag (Anlage 1 Kap. Il Sachgebiet C Abschnitt 111 Nr. 4 Buchst. b) eine weitere Nutzung der Personenkennzeichen (PKZ) des Meldedatenbestandes nicht mehr zulässig. Denn mit dem PKZ hatte die DDR-Staatsgewalt einen Schlüssel zu den Daten ihrer Bürger auf allen Ebenen und Bereichen des sozialen Zusammenlebens. Mit Hilfe des PKZ wurden alle Datenfelder verknüpft, Persönlichkeitsbilder erstellt und unmenschliche Repressalien ermöglicht. Die DDR hielt die Menschen mit Hilfe der PKZ im »informationellen Würgegriff«.

Der Bundesbeauftragte für die Stasi-Unterlagen sieht jedoch die weitere Nutzungsmöglichkeit als für seine Aufgabenerfüllung erforderlich an, weil die PKZ seine Recherche in den Unterlagen des ehemaligen Ministeriums für Staatssicherheit erleichtere und hierdurch Personenverwechslungen faktisch ausgeschlossen werden könnten. Die an der Sitzung der Arbeitsgruppe »Datenschutz in den neuen Bundesländern<< 4. März 1993 beteiligten Landesbeauftragten für den Datenschutz Berlin, Brandenburg und Sachsen vertreten zur weiteren Nutzung des ZER-Meldedatenbestandes folgenden Standpunkt:

1. Die Sicherstellung des Meldedatenbestandes (Zuständigkeit für die weite Aufbewahrung, Lesbarmachung, kompatible Formatierung) kann in einem Verwaltungsabkommen zwischen den fünf neuen Ländern und Berlin geregelt werden.
2. Hingegen bedarf die Nutzung des Meldedatenbestandes einer gesetzlichen Grundlage, ähnlich dem Krebsregistersicherstellungsgesetz, die von dem für den jeweiligen Bereich zuständigen Gesetzgeber zu erlassen ist und bestimmten Anforderungen genügen muß (abschließende Aufzählung der späteren Nutzer so auf die Nutzung abgestimmter Datensatz, der hierzu übermittelt werden soll).

1.5.Verwendung von Stasi-Unterlagen

1.5.1
Im Zusammenhang mit dem privaten Dresdner »Forschungszentrum zu den Verbrechen des Stalinismus« habe ich die Verwendung von Dokumenten des MfS unter datenschutzrechtlichen Gesichtspunkten überprüft. Es. handelte sich um Informationen, die vom Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemali-

gen DDR (Bundesbeauftragter) an die Betroffenen herausgegeben worden sind. Fraglich könnte nämlich sein, ob die an den Betroffenen nach § 3 Abs. 2 StasiUnterlagen-Gesetzes (StUG) herausgegebenen Unterlagen einer Verwendungsbeschränkung unterliegen mit der Folge, daß dritten Personen oder Einrichtungen (z. B. Forschungszentren zur Aufarbeitung der DDR-Vergangenheit) eine Zusammenführung solcher vom Bundesbeauftragten herausgegebenen Unterlagen zu neuen Datensammlungen verwehrt wäre. Auch tauchte die Frage auf, ob dieserart entstandene Akten oder Dateien als Altdaten im Sinne des Sächsischen Datenschutzgesetzes gelten könnten. Schließlich besteht die Möglichkeit, daß vom Bundesbeauftragten anonymisierte Daten deanonymisiert werden, wenn die vom Bundesbeauftragten an den Betroffenen herausgegebenen Akteninformationen mit weiteren, beim Forschungszentrum vorhandenen Informationen abgeglichen und zusammengeführt werden.

Ich habe diese Problematik auch wegen mehrerer Anfragen eingehend untersucht und bin nach z. T. kontroverser Diskussion mit dem Bundesbeauftragten für StasiUnterlagen mit dem Bundesminister des Innern sowie mit den betroffenen Kreisen zu folgender Auffassung gelangt:

- Die vom Bundesbeauftragten herausgegebenen Informationen aus Stasi-Unterlagen können vom Adressaten im Rahmen der allgemeinen Gesetze und der vom Stasi-Unterlagen-Gesetz getroffenen Zweckbindung weiterverwendet werden.
- Das Sammeln der vom Bundesbeauftragten zur Verfügung gestellten Informationen durch sogenannte »Forschungszentren« gehört nicht zu meinem Zuständigkeitsbereich; diese Informationen sind wohl keine Altdaten im Sinne von § 35 SächsDSG.
- Die Duplikate von Akten des Staatssicherheitsdienstes, die vom Bundesbeauftragten auf Antrag herausgegeben worden sind, fallen nicht unter den Unterlagenbegriff des § 6 StUG.

1.5.2

Am Jahresende stand diese Problematik erneut im Blickpunkt der Öffentlichkeit: Eine Dresdner Boulevardzeitung veröffentlichte personenbezogene Daten der hauptamtlichen Mitarbeiter der MfS-Bezirksverwaltung Dresden. Der listenmäßige Abdruck beruhte auf einer zuvor publizierten Ausarbeitung des »Bürgerkomitees Bautzner Straße e.V.«, welches ihm vom Bundesbeauftragten für die Stasi-Unterlagen überlassene Informationen zusammengestellt hatte.

Einige der von der Veröffentlichung betroffene ehemalige hauptamtliche Mitarbeiter des Staatssicherheitsdienstes haben sich daraufhin an mich gewandt und um datenschutzrechtlichen Rat gebeten. Ich habe ihnen mitgeteilt, daß § 34 Abs. 1 i. V. mit § 32 Abs. 3 Nr. 2 StUG der Presse auch ohne Einwilligung die Verwendung - mithin auch die Veröffentlichung - von Unterlagen mit personenbezogenen Informationen über hauptamtliche und inoffizielle Mitarbeiter des Staatssicherheitsdienstes erlaubt.

Allerdings darf die Veröffentlichung nur erfolgen, wenn hierdurch keine wiegenden schutzwürdigen Interessen der genannten Personen beeinträchtigt werden. Für die Frage, ob solche überwiegenden Interessen durch diese Veröffentlichung beeinträchtigt worden sind, sind die ordentlichen Gerichte zuständig. Dagegen ist für die Klärung der Frage, ob der Bundesbeauftragte für die Stasi-Unterlagen zulässigerweise die Unterlagen zur Verfügung gestellt hat, der Verwaltungsrechtsweg zu beschreiten.

Bürger, die Fragen zur Verwendung ihrer personenbezogenen Daten durch den ehemaligen Staatssicherheitsdienst haben, können sich nunmehr auch an den Sächsischen Landesbeauftragten für die Stasi-Unterlagen wenden, mit dessen Aufgabenbereich meine Arbeit Überschneidungen haben wird (vgl. auch Nr. 1.3).

1.6 Nicht-öffentlicher Bereich

Immer wieder wenden sich Bürger an mich, die sich durch die Datenverarbeitung privater Stellen in ihren Rechten verletzt fühlen. Diesen Eingaben kann ich jedoch nicht nachgehen, weil sich meine Kontrollkompetenz nach dem Sächsischen Datenschutzgesetz auf den Bereich der öffentlichen Stellen des Freistaates Sachsen beschränkt. Für die Kontrolle der nichtöffentlichen Datenverarbeitung sind in Sachsen gemäß § 38 Abs. 6 Bundesdatenschutzgesetz in Verbindung mit der einschlägigen Verordnung der Sächsischen Staatsregierung vom 27.8. 1991 (SächsGVBI. S.324) die Regierungspräsidien Dresden, Leipzig und Chemnitz zuständig. Somit muß ich- sofern das Einverständnis vorliegt - die Eingaben der Petenten an die Datenschutzkontrollinstanzen bei den Regierungspräsidien abgeben.

Ich habe leider festgestellt, daß die Regierungspräsidien in diesem Bereich ihrer Zuständigkeit noch nicht die gebotene Arbeitsfähigkeit besitzen. Deshalb habe ich das fachaufsichtsführende Sächsische Staatsministerium des Innern an seine Verantwortung erinnert, den Auftrag des Bundesdatenschutzgesetzes auszuführen und eine funktionierende Datenschutzkontrolle im privaten Bereich zu gewährleisten. Unzureichende Personal- und Finanzausstattung darf nicht dazu führen, daß dem Bürger gesetzlich eingeräumte Kontrollmöglichkeiten faktisch nicht zur Verfügung stehen. Ich werde die Problematik weiter im Auge behalten.

1.7 Aufgaben des behördlichen Datenschutzbeauftragten

Immer wieder wird die Frage gestellt, ob sächsische öffentliche Stellen einen behördeninternen Datenschutzbeauftragten bestellen müssen und welche Aufgaben dieser ggf. hat.

Zu diesen Fragen habe ich mich ausführlich in der Bekanntmachung vom 21.8. 1992 über »Hinweise zu den Aufgaben eines internen Datenschutzbeauftragten öffentlicher Stellen« im Sächsischen Amtsblatt Nr. 25/1992, S. 1295 geäußert. Diese Bekanntmachung (siehe Nr. 16.1.2) möchte ich in Erinnerung bringen.

1.8. Gleichstellung von Mann und Frau im öffentlichen Dienst

Die Parlamentarische Staatssekretärin für die Gleichstellung von Mann und Frau hat mir Entwürfe eines »Gesetzes zur Gleichstellung von Frauen und Männern durch Förderung der beruflichen Chancen von Frauen und der Vereinbarkeit von Familie und Beruf im öffentlichen Dienst im Freistaat Sachsen (SächsGIStG)« zur Stellungnahme übersandt.

Allgemeine verfassungsrechtliche Bedenken gegen die vorgesehene Aufarbeitung der bislang gewachsenen Unterrepräsentation der Frauen (auf gewissen Gebieten aber auch der Männer -z. B. in Kindergärten) durch deren Bevorzugung bei gleicher Eignung habe ich wegen fehlender Zuständigkeit nicht zu kommentieren.

Meine Anregung, die Verschwiegenheitspflichten der Gleichstellungsbeauftragten im Gesetz zu regeln, wurde aufgegriffen. Ich finde es auch gut, daß die Gleichstellungsbeauftragte nur mit Einwilligung der Bediensteten deren Personalakten einsehen darf.

Nachdrückliche Bedenken habe ich aber gegen die vorgesehene *umfassende* Unterrichtungs und Erörterungspflicht der Gleichstellungsbeauftragten vor Personalentscheidungen sowie gegen ihr Recht erhoben, ohne Einwilligung der Betroffenen Bewerbungsunterlagen und sonstige Akten einsehen zu dürfen. Insofern vermochte ich dem Gesetzentwurf nicht zuzustimmen.

Ich werde mich an der weiteren Entwicklung des Gesetzesvorhabens beteiligen.

2 Landtag; Verhältnis Parlament - Regierung

2.1 Ausübung des Informationsrechts durch den Landtag

Einige Antworten der Staatsregierung auf parlamentarische Anfragen enthielten den Hinweis, "datenschutzrechtliche Gründe" stünden einer weiteren Beantwortung entgegen. So hat der Landwirtschaftsminister die Antwort auf die Frage nach den Eigentums- u. Förderungsverhältnissen der großen milchverarbeitenden Betriebe unter Hinweis auf Datenschutz verweigert.

Durch diese pauschalisierende Verwendung des Datenschutzbegriffs sah ich mich zu einer Klarstellung gegenüber dem Präsidenten des Landtages und dem Ministerpräsidenten veranlaßt.

Der nach Art. 51 Abs. 1 Sächsische Verfassung gewährleistete Anspruch des Parlaments, daß seine Fragen an die Staatsregierung unverzüglich und vollständig beant-

wortet werden, findet seine Grenze im Recht der Staatsregierung nach Art. 51 Abs. 2 Sächsische Verfassung, die Beantwortung von Fragen ablehnen zu können, wenn diese den Kernbereich exekutiver Eigenverantwortung berühren oder einer Beantwortung gesetzliche Regelungen, Rechte Dritter oder überwiegende Belange des Geheimschutzes entgegenstehen. Dies bedeutet, daß die den Schutz der Persönlichkeit des einzelnen bezweckenden Rechtsvorschriften (Gesetze, Rechtsverordnungen) beschnitten werden können, indem die Verfassungsnorm des Art. 51 die Anwendung dieser Rechtsvorschriften in das Ermessen der Regierung stellt: danach wäre zunächst von der prinzipiellen Zulässigkeit der Preisgabe - auch sensibler - personenbezogener Informationen durch die Regierung auszugehen.

Damit - so scheint es - liefen sämtliche Regelungen zum Schutz der Persönlichkeit ins Leere, wenn nicht der sächsische Verfassungsgeber mit Art. 33 dem Recht auf informationelle Selbstbestimmung eine explizite Verankerung verliehen hätte.

Das hierdurch auftretende Spannungsverhältnis zwischen dem Recht des Einzelnen auf Schutz seiner Daten und dem Informationsrecht des Parlaments löst das Bundesverfassungsgericht: Dem Grundgedanken der "Herstellung praktischer Konkordanz" folgend hat es festgestellt, daß grundrechtlicher Datenschutz zwar auch gegenüber den Befugnissen parlamentarischer Gremien besteht. Deren Beweiserhebungsrecht rangiert aber gleichermaßen auf der Ebene des Verfassungsrechts; beide Rechte müssen deshalb im konkreten Fall einander so zugeordnet werden, daß beide so weit wie möglich ihre Wirkungen entfalten (BVerfGE 67, 143 f.). Für das Bundesverfassungsgericht bedeutet dies, daß das Kontrollrecht des Parlaments wegen seiner Bedeutung für die parlamentarische Demokratie und für das Ansehen des Staates nur dann hinter dem Persönlichkeitsrecht des Einzelnen zurücktritt, wenn Informationen in Rede stehen, "deren Weitergabe wegen ihres streng persönlichen Charakters für die Betroffenen unzumutbar ist" (BVerfGE 67, 144); dies sind nach dem Volkszählungsurteil Informationen aufgrund "intimer Angaben und Selbstbezichtigungen" (BVerfGE 65, 46).

Damit wird deutlich, in welch engen Grenzen die Berufung auf "datenschutzrechtliche Gründe" oder "Datenschutz" als Rechtfertigung einer Auskunftsverweigerung statthaft ist: Der - hier allein in Frage kommende - Kernbereich der Privatsphäre (intime Angaben und Selbstbezichtigungen) dürfte nur in seltenen Fällen Gegenstand einer Regierungsantwort sein. Bei allen anderen Fragekonstellationen wird das Grundrecht auf Schutz der Persönlichkeit nicht eine Auskunftsverweigerung der Regierung gegenüber dem Parlament tragen - vielmehr birgt der in diesen Fällen unzulässig vorgebrachte Hinweis auf "den Datenschutz" die Gefahr, den institutionalisierten Schutz der Persönlichkeitssphäre zu diskreditieren.

Dies zu vermeiden sollte gleichermaßen Anliegen von Parlament und Regierung sein.

Unterhalb einer Verweigerung der Auskunft ist zu differenzieren:
Wenn das Parlament - dies gilt auch für Gemeinderäte - private Daten außerhalb des Kernbereichs der Persönlichkeit von der Exekutive erfragt (z.B. ob die Ehefrau eines

Beamten Geschäfte in dessen Verantwortungsbereich tätigt oder wie hoch der Verkaufserlös war, den ein Bürger für eine Liegenschaft erzielt hat), so besteht die Möglichkeit, daß die Antwort in nichtöffentlicher Sitzung des Plenums, vor einem Ausschuß oder sogar mit besonderer Geheimhaltungsverpflichtung erteilt wird.

2.2 Parlamentsdokumentationssystem

Die Verwaltung des Sächsischen Landtages hat mich gebeten zu prüfen, ob die im Rahmen des Parlamentsdokumentationssystems erstellte Datenbank jedermann zugänglich sein darf. Ich habe hierzu geäußert, daß Datenbestände des Parlamentsdokumentationssystems über Plenarprotokolle, Drucksachen und die im Volkshandbuch enthaltenen personenbezogenen Informationen über Abgeordnete keinen Zugangsbeschränkungen unterliegen. Dagegen ist die Zulässigkeit des freien Zugangs zu Ausschußprotokollen von der (seltenen) Öffentlichkeit der Ausschußsitzungen abhängig. In diesem Zusammenhang ist auf § 28 der Geschäftsordnung des Sächsischen Landtages hinzuweisen, der das Persönlichkeitsrecht schützt.

2.3 Nennung von Namen Belasteter im Plenum

Im Oktober 1992 habe ich gegenüber dem Sächsischen Wissenschaftsminister eine förmliche Beanstandung ausgesprochen. Dieser hatte in einer öffentlichen Sitzung des Landtages sieben Namen von Hochschullehrern einer Sächsischen Universität genannt und bei drei Professoren deren Tätigkeit als Mitarbeiter des Ministeriums für Staatssicherheit, bei vier Professoren deren Repressionen gegen Mitarbeiter oder Kollegen geschildert.

Der Minister hat damit in das Grundrecht auf informationelle Selbstbestimmung der Professoren eingegriffen. Die Bekanntgabe der Namen war zur Erfüllung seiner Aufgaben als Staatsminister nicht erforderlich. Auch im verständlichen Bemühen um politische Aufarbeitung des DDR-Unrechts ist eine solche bloßstellende Veröffentlichung von Fakten in unmittelbarer Verbindung mit Namen unangemessen. Der verfassungsrechtliche Begriff der "Erforderlichkeit" ist nicht gleichzusetzen mit politischem Erfordernis.

Der Staatsminister hat sich dahingehend gerechtfertigt, die Unterrichtung des Landtags sei in dieser Deutlichkeit notwendig gewesen, da
- die Namen der Professoren schon früher in der Presse genannt worden seien,
- der falsche Eindruck entstanden sei, der Freistaat entlasse aus sachfremden Erwägungen auch unbelastete hochqualifizierte Wissenschaftler,
- das Kontroll- und Informationsrecht des Parlaments höher zu gewichten sei als das Geheimhaltungsinteresse der Hochschullehrer.

Nach der Rechtsprechung des Bundesverfassungsgerichts hat das Kontrollrecht des Parlaments grundsätzlich nur dann hinter dem Persönlichkeitsrecht des einzelnen zu-

rückzutreten, wenn eine Weitergabe von Informationen wegen ihres streng persönlichen Charakters für die Betroffenen unzumutbar ist (intime Angaben und Selbstbezichtigungen). Indes ging es hier nicht um diese Grundsatzfrage, weil das Parlament eine solche explizite Frage nicht gestellt hatte, sondern es ging darum, ob einer politischen Rechtfertigung und einer (nur daraus abgeleiteten) angeblichen Informationspflicht der Regierung nur durch die Übermittlung ausschließlich personenbezogener Detailinformationen (also mit Namensnennung) genügt werden konnte und ob aus Gründen eines politischen Vorteils in Grundrechte eingegriffen werden darf. Dies war zu verneinen. Dem Minister war es unbenommen, aus politischen Gründen und zur Unterrichtung des Parlaments ohne Namensnennung ganz konkrete Gründe für Kündigungen in seinem Geschäftsbereich aufzuführen. Es wäre ausreichend und angemessen gewesen, wenn die geschilderten Sachverhalte vorgetragen worden wären. Hätte der Minister dennoch geglaubt, sich ohne Namensnennung nicht ausreichend rechtfertigen zu können, hätten sich ein Antrag auf Ausschluß der Öffentlichkeit oder eine nichtöffentliche Ausschußsitzung angeboten.

Festzustellen bleibt, daß die persönlichen Abqualifizierungen, mögen sie auch dem überwiegenden Teil der Öffentlichkeit im Hinblick auf in 40 Jahren erlittenes Unrecht als gerechtfertigt erscheinen, Folgen haben, die in nachteiliger Weise weit in die private, bürgerliche Existenz der Betroffenen hineinwirken.

Wenn wir nicht vorhätten, den Prozeß der personellen Erneuerung mit streng rechtsstaatlichen Regeln durchzuführen, dürften wir ihn gar nicht erst begonnen haben.

3 EG-Richtlinie zum Datenschutz

Dem Ministerrat der EG liegt seit 15. Oktober 1992 ein überarbeiteter Vorschlag für eine EG-Richtlinie "Zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" (KOM (92) 42 endg. - SYN 287) vor. Damit hat die EG-Kommission auf die Änderungsvorschläge des Europäischen Parlaments zu ihrem Vorschlag aus dem Jahre 1990 reagiert.
Die EG-Richtlinie soll nach Öffnung der Binnengrenzen gewährleisten, daß ein grenzüberschreitender Austausch von Daten natürlicher Personen nicht mehr wegen unterschiedlicher nationaler Datenschutzgesetze unterbunden werden kann. Dabei wird das Ziel verfolgt, ein in allen Mitgliedsstaaten gleiches, hohes Datenschutzniveau einzuführen.
Der Richtlinienvorschlag unterwirft die öffentliche und die private Datenverarbeitung grundsätzlich denselben Regeln; damit würde eine - im deutschen Recht bisher bestehende - Unterscheidung zwischen öffentlichem und privatem Bereich aufgehoben.
Der Vorschlag enthält in Artikel 8 strikte Beschränkungen der Verarbeitung empfindlicher Daten: So sollen in den Mitgliedsstaaten Angaben über rassische und ethnische Herkunft, die politische Meinung, religiöse, philosophische oder moralische Überzeugung sowie Informationen über Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben nicht verarbeitet werden dürfen.

Allerdings weist der Richtlinienvorschlag in seiner jetzigen Fassung noch Änderungsbedarf auf:
Die Erschwernisse für die Datenerhebung und ihre Übermittlung an die öffentlich-rechtlichen Religionsgesellschaften müssen wegen deren wichtiger öffentlicher Aufgaben abgebaut werden.
Es sollte klargestellt werden, daß es den Mitgliedsstaaten unbenommen bleibt, im einzelstaatlichen Recht für die Datenverarbeitung ohne grenzüberschreitenden Bezug ein höheres Schutzniveau zu gewährleisten. Dies ist wichtig, weil sonst einige ausgefeilte, bereichsspezifische Datenverarbeitungsregeln des deutschen Rechts keine Anwendung mehr finden könnten.
In Art. 33 der Richtlinie bleibt unklar, ob die EG-Kommision außerhalb eines Gesetzgebungsverfahrens die Kompetenz erhalten soll, bereichsspezifische Regelungen für den Datenschutz zu treffen. Dies sollte wegen des Subsidiaritätsprinzips den Nationen und Regionen tunlichst überlassen bleiben.
Es muß sichergestellt werden, daß sich private oder öffentliche (z.B. polizeiliche) Stellen durch eine Datenverarbeitung in Drittländern nicht den Bindungen des gemeinschaftsrechtlichen Datenschutzes entziehen können.
Darüber hinaus muß die Unabhängigkeit der nationalen Datenschutzkontrollbehörden von Regierung und Exekutive unangetastet bleiben. Für die deutschen Datenschutzbehörden ergeben sich aber Probleme, weil der Richtlinienvorschlag den Kontrollbehörden Exekutiv- und Anordnungsbefugnisse gibt, welche die deutschen Datenschutzbeauftragten bislang nicht besitzen. Jede hoheitsrechtliche Verwaltungsbefugnis bedarf jedoch einer parlamentarischen Kontrolle.
Nach dem bisherigen Entwurf der Richtlinie wird es den gesetzlich besonders geschützten internen Datenschutzbeauftragten in Betrieben und Behörden nicht mehr geben.
Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer Sitzung vom 16./17. Februar 1993 einen Beschluß (s. Nr. 16.2.7) gefaßt, mit dem sie gegenüber der EG-Kommission sowie den in Deutschland mit der Richtlinie befaßten Ministerien und Gremien ihre datenschutzrechtlichen Forderungen beschreibt, damit diese bei der weiteren Beratung im EG-Ministerrat berücksichtigt werden.
Seit Dienstantritt habe ich mich in Brüssel und in Hamburg über die Datenschutzgesetzgebung der EG informiert; 1993 muß hier ein Schwerpunkt meiner Arbeit gesetzt werden.

4 Medien

Das Datenschutzgesetz enthält keine spezielle Vorschrift, welche die Verwendung personenbezogener Informationen durch die Medien regelt. Soweit diese Daten durch Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Fernsehens ausschließlich zu eigenen publizistischen Zwecken verarbeitet werden, gilt ein "Medienprivileg", das der wertsetzenden Bedeutung des Art. 5 Abs. 1 GG ("Pressefreiheit") entspricht. Dieses Privileg muß aber das kollidierende Grundrecht auf Datenschutz, also das Persönlichkeitsrecht, berücksichtigen und im Einzelfall restriktiv ausgelegt werden. Betroffenen steht im Fall der Verletzung ihres Persönlichkeitsrechts u. U. ein

Anspruch auf Gegendarstellung, Unterlassung, Widerruf bzw. Schadensersatz zu, außerdem können sie Strafanzeige erstatten. Die Medien sind Privatunternehmen, die nicht meiner Kontrolle unterliegen; sie haben üblicherweise interne Datenschutzbeauftragte mit weitreichenden Kompetenzen (siehe z. B. § 42 des Staatsvertrages über den MDR vom 30.Mai 1991).

Materiell ist der Datenschutz im öffentlichen und im privaten Rundfunk in § 28 des Staatsvertrages über den Rundfunk im vereinten Deutschland (Gesetz vom 19. Dezember 1991) geregelt und für das ZDF in §§ 16-18 des ZDF-Staatsvertrages. Das Privatrundfunkgesetz vom 27. Juni 1991 regelt in §§ 44, 45 den Schutz personenbezogener Informationen: Der bei der aufsichtsführenden Landesmedienanstalt zu bestellende Datenschutzbeauftragte hat nach dieser Vorschrift, die von mir vorgeschlagen wurde, mit mir "zusammenzuarbeiten". Auf diese gemeinsame Arbeit werde ich Wert legen.

Soweit § 4 des Landespressegesetzes ein Informationsrecht der Presse gegenüber den Behörden in Sachsen regelt (dies gilt auch für Bundesbehörden), wurde auf meine Anregung, die von der CDU-Fraktion aufgegriffen wurde, ein Auskunftsverweigerungsrecht des Behördenleiters u. a. für den Fall statuiert, daß Vorschriften über den Persönlichkeitsschutz (also z.B. § 15 SächsDSG) entgegenstehen oder durch die Auskunft an die Presse ein anderweitiges schutzwürdiges privates Interesse verletzt würde.
Soweit ausschließlich dienstbezogene Daten von Mitarbeitern im öffentlichen Dienst z. B. in der Presse veröffentlicht werden, ist das Grundrecht auf informationelle Selbstbestimmung nicht berührt, weil "der Staat" (und "die Gemeinde") und folglich die ihn verkörpernden Personen - wohlgemerkt: in dieser dienstlichen Eigenschaft - nicht Träger von Grundrechten sein können (Unterscheidung zwischen Amt und Person).

5. Inneres

5.1 Personalwesen

5.1.1 Rechtliche Entwicklung

Durch das Neunte Gesetz zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 ist im Beamtenrechtsrahmengesetz die Grundlage für Regelungen zum Umgang mit den Personalakten der Beamten in den einzelnen Bundesländern geschaffen worden. Zu begrüßen ist, daß in das Beamtengesetz für den Freistaat Sachsen vom 17. Dezember 1992 die betreffenden Vorschriften sowie die Aufbewahrungsvorschrift für die Personalakten der Bundesbeamten auf meine Anregung hin übernommen worden sind.
Damit sind nunmehr umfassend geregelt:

- Die Pflicht des Dienstherrn zur Führung von Personalakten sowie Inhalt und Gliederung der Personalakte,
- die Behandlung von Beihilfeunterlagen,
- das Anhörungs- und Personalakteneinsichtsrecht des Beamten sowie sein Recht auf Gegendarstellung,
- die Vorlage der Personalakte und die Erteilung von Auskünften an Dritte,
- die Aufbewahrungsfrist,
- die automatisierte Verarbeitung und Nutzung von Personalaktendaten.

Da der Inhalt einer Personalakte bisher nicht genau festgelegt war, ist es ein Fortschritt, daß das Gesetz nunmehr selbst definiert, welche Unterlagen zur Personalakte gehören - nämlich alle Unterlagen, einschließlich der in Dateien gespeicherten, die den Beamten betreffen und in einem inneren unmittelbaren Zusammenhang mit seinem Dienstverhältnis stehen. Gemeint sind damit auch "behördeninterne Vorgänge", wenn sie Entscheidungen zum Dienstverhältnis vorbereitet haben (Bundesverwaltungsgericht). Damit wird die Personalakte in ihrem materiellen Inhalt definiert. Personalaktendaten sind danach nicht nur solche Daten, die sich tatsächlich in der Personalakte befinden (formelle Personalakte), sondern auch bislang in anderen Akten, Karteien oder sonstigen automatisiert geführten Personaldaten- und Informationssystemen enthaltene Informationen.

Leider sehen die Tarifverträge für die Arbeiter und Angestellten des öffentlichen Dienstes mit Ausnahme des Anhörungsrechts entsprechend klar und detailliert formulierte Regelungen nicht vor. Die Tarifparteien sollten sich tunlichst auch mit diesem Thema befassen.

5.1.2 Informationelles Selbstbestimmungsrecht im öffentlichen Dienst

In einer Eingabe hat sich der Betroffene dagegen gewandt, daß seine Dienststelle von sämtlichen Bediensteten ein (polizeiliches) Führungszeugnis zur Vervollständigung der Personalakte verlangt. Außerdem hat ihn die Frage nach den Wohnsitzen der letzten 10 Jahre gestört. Der Petent befürchtete eine mißbräuchliche Nutzung der Führungszeugnisse durch seine Behörde und fühlte sich in seinem informationellen Selbstbestimmungsrecht beeinträchtigt.

Ich habe die Eingabe wie folgt bewertet:
Nach § 70 Sächsisches Beamtengesetz haben sich Beamte in einem Diensteid zur Verfassungs- und Gesetzestreue zu bekennen. § 6 BAT schreibt ein diesbezügliches Gelöbnis für Angestellte des öffentlichen Dienstes vor. Diese Bestimmungen entsprechen Art. 20, 28 und 33 Abs. 4 Grundgesetz, wonach die Zugehörigkeit zum öffentlichen Dienst eine Bejahung der freiheitlichen-demokratischen Grundordnung in Bund und Ländern voraussetzt. Die in Art. 33 Abs. 4 Grundgesetz festgelegte Treuepflicht gegenüber der verfassungsgemäßen staatlichen Ordnung führt zu dem

Ergebnis, daß im öffentlichen Dienst Beschäftigte Einschränkungen des Rechts auf informationelle Selbstbestimmung hinnehmen müssen, was nicht zuletzt auch in Art. 119 Sächsische Verfassung zum Ausdruck kommt.

Selbstverständlich gehört es zu den Aufgaben eines öffentlich-rechtlichen Arbeitgebers, sich zu überzeugen, ob seine Bediensteten die Gewähr für verfassungs- und gesetzestreue Amtsausübung bieten. Die vom Dienstherrn geforderte Vorlage von Führungszeugnissen sämtlicher Mitarbeiter ist eine von mehreren Möglichkeiten, sich von der Zuverlässigkeit der Behördenbediensteten zu überzeugen. Auch die Frage nach den Wohnanschriften der letzten 10 Jahre dient letztlich dieser Zuverlässigkeitsprüfung (z. B. Anfrage an Gauck-Behörde).

Die nicht näher begründete Behauptung des Petenten, daß ein Mißbrauch der Führungszeugnisse "vorprogrammiert" sei, entbehrt im Hinblick auf Art. 20 Abs. 3 Grundgesetz (die vollziehende Gewalt ist an Gesetz und Recht gebunden) jeglicher Grundlage.

5.1.3 Zuschalten eines Lautsprechers bei Dienstgesprächen

In einer Eingabe wurde ich darauf hingewiesen, daß bei einem Dienstgespräch die angerufene Dienststelle durch Zuschalten eines Lautsprechers Dritten die Kenntnisnahme des Gesprächsinhalts ermöglichte, ohne den Anrufer vorher von dieser Maßnahme zu verständigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 1./2. Oktober 1992 zum Datenschutz bei internen Telekommunikationsanlagen (s. Nr. 16.2.4) bereits gefordert, daß das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein darf. In diesem Sinne hatte das Bundesverfassungsgericht in seinem Beschluß vom 19.12.1991 - BvR 382/85 (NJW 1992, Heft 13, S. 815) wie folgt entschieden:
"Der grundrechtliche Schutz des gesprochenen Wortes kann nicht durch die bloße Kenntnis von einer Mithörmöglichkeit beseitigt werden. Die Benutzung eines Diensttelefons allein rechtfertigt daher nicht den Schluß, damit sei dem Sprechenden eine Erweiterung des Adressatenkreises gerade um den Arbeitgeber oder dessen Vertreter gleichgültig."
Weiterhin sieht es das Bundesverfassungsgericht als einen Verstoß gegen Art. 2 Abs. 1 GG (Recht auf freie Entfaltung der Persönlichkeit) i. V. m. Art. 1 Abs. 1 GG (Menschenwürde) an, wenn Telefongespräche, die der Arbeitnehmer von einem Dienstapparat aus führt, vom Vorgesetzten von vornherein aus dem durch das allgemeine Persönlichkeitsrecht gewährten Schutz herausgenommen werden. Das Recht des Betroffenen am *eigenen Wort,* das als Ausprägung des allgemeinen Persönlichkeitsrechts anerkannt ist, umfaßt - so das Bundesverfassungsgericht - die Befugnis des Menschen, selbst zu bestimmen, ob seine Worte einzig seinem

Gesprächspartner, einem bestimmten Kreis oder der Öffentlichkeit zugänglich sein sollen (vgl. BVerfGE 54, 148 (155) = NJW 1980, 2070).

Aus alledem folgt, daß ohne eindeutige und rechtzeitige Ankündigung, die es dem Betroffenen ermöglicht zu widersprechen, das Einschalten einer Mithöreinrichtung (z. B. Lautsprecher) oder eine Aufschaltung (auf bereits zustandegekommene Verbindungen), verfassungswidrig und damit unzulässig wäre.

5.1.4 Akteneinsicht der Beteiligten bei Konkurrentenklagen

Datenschutzbeauftragte der alten Bundesländer haben auf eine Situation bei Konkurrentenklagen hingewiesen, die sich verstärkt in den neuen Ländern ergeben kann. Konkurrentenklagen erhalten eine datenschutzrechtliche Problematik in allen Fällen, in denen sich mehrere Personen für ein Amt innerhalb einer Behörde bewerben, weil das Ergebnis des auf die Bewerbungen folgenden Auswahlverfahrens anschließend allen unterlegenen Bewerbern mitgeteilt wird. Diese haben das Recht, eine Verletzung des Art. 33 Abs. 2 GG gerichtlich geltend zu machen, um auf diese Weise selbst zur Einstellung/Beförderung zu kommen. Kommt es zu einem solchen Rechtsstreit, haben sämtliche Beteiligte des Verfahrens in entsprechender Anwendung des § 100 Abs. 1 Verwaltungsgerichtsordnung (VwGO) das Recht auf Akteneinsicht. Dieses Recht erfaßt die gesamten dem Gericht zur Entscheidung vorliegenden Unterlagen und Urkunden, einschließlich der in diesem Rechtsstreit besonders interessierenden Personalakten.

Ich habe daher den Sächsischen Staatsministerien u. a. folgendes mitgeteilt:

Da es bei der Konkurrentenstreitigkeit gerade um die Frage der besseren Eignung, Befähigung und fachlichen Leistung des abgelehnten Mitbewerbers geht, kann auf die Anforderung der Personalakten des Klägers und seiner Konkurrenten seitens des Gerichts grundsätzlich nicht verzichtet werden. Es ist aber zu berücksichtigen, daß nicht alle Unterlagen in den Personalakten den jeweiligen konkreten Streitgegenstand betreffen, also streitentscheidend sind. Gerade diese Daten müssen aus datenschutzrechtlichen Gründen vor der Einsichtnahme durch den jeweiligen Konkurrenten und seinen Anwalt (gemäß § 100 Abs. 1 VwGO; bei Angestellten und Arbeitern gilt die Zivilprozeßordnung) geschützt werden, weil ihre Bekanntgabe für die Gerichtsentscheidung nicht erforderlich ist. So dürften beispielsweise in Beförderungsfällen die "Gauck-Unterlagen" als getrennt zu führende Personal-Aktenhefte nicht zum Streitgegenstand gehören. Die Entscheidung, welche Daten im einzelnen zum Streitgegenstand gehören und daher zur Einsicht freigegeben sind, darf allerdings nach herrschender Rechtsprechung nur das Gericht fällen, da dieses über die Sach- und Rechtslage unter Berücksichtigung aller Gesichtspunkte, die es für wichtig hält, zu urteilen hat.
Das Gericht sollte daher, bevor es das Recht zur Akteneinsicht gewährt, den Streitgegenstand unter Abwägung zwischen dem Persönlichkeitsrecht des Einzelnen

und dem Grundsatz der Parteiöffentlichkeit des Prozesses festlegen. Wegen der Rechtsunsicherheit auf diesem Gebiet habe ich das Staatsministerium für Justiz zunächst gebeten, im Bundesrat auf eine Änderung der VwGO im Hinblick auf den Umgang mit Personaldaten hinzuwirken. Unter Berücksichtigung der *bestehenden* Gesetzeslage habe ich bei den sächsischen Staatsministerien folgende Verfahrensweise angeregt und gebeten, die nachgeordneten Behörden entsprechend zu unterrichten:
Auf Anforderung des Gerichts ist die Behörde verpflichtet, sämtliche Akten vorzulegen. Gelangen auf diese Weise personenbezogene Daten an das Gericht und meint die Behörde, daß ein Bezug zum Streitgegenstand fehlt, so soll sie mittels eines Antrags darauf hinwirken, daß diese Unterlagen von der übrigen Akte getrennt und zurückgegeben werden. Die Entscheidung über die Rückgabe (also über den Streitgegenstand) steht allerdings allein dem Gericht zu.
Das Justizministerium hat mich dann jedoch mit Schreiben vom 3. März 1993 davon überzeugt, daß das Gericht gehalten ist, die nicht entscheidungserheblichen Personalaktenteile auszusondern, an die Behörde zurückzugeben und bei seiner Entscheidung nicht zu berücksichtigen. Dem Kläger wird Einsicht nur in die der Entscheidung zugrunde liegenden Unterlagen gewährt; der datenschutzrechtlich unzulässige Einblick in die vollständigen Personalakten des Konkurrenten wird so verhindert.

Unter diesen Umständen halte ich eine Änderung der VwGO nicht für erforderlich.

5.1.5 Personalbogen

Wegen mehrerer Eingaben und Anfragen öffentlicher Stellen habe ich mich mit dem Inhalt von Personalbogen befaßt. Dabei habe ich festgestellt, daß bereits im Bewerbungsverfahren - also zu einem Zeitpunkt, zu dem noch ungewiß ist, ob ein Dienstverhältnis überhaupt zustande kommt - mit dem Personalbogen Daten erhoben werden, deren Kenntnis nicht oder erst für das spätere Dienstverhältnis erforderlich ist.

Ich habe auf die Unzulässigkeit eines solchen Verfahrens hingewiesen und empfohlen, solche Angaben zu kennzeichnen, die der Dienststelle erst bei Einstellung mitzuteilen sind: Die Daten des Ehegatten und der Kinder, soweit sie sich auf die Höhe der Bezüge auswirken (möglichst unter Verwendung eines separaten Fragebogens, der den Besoldungsunterlagen zuzuordnen ist); Angaben zu Nebentätigkeiten; Bankverbindung usw.

Als generell unzulässig habe ich folgende Fragen in den Personalbogen beanstandet:
- Zweiter Wohnsitz,
- Angaben zum Familienstand, die über "verheiratet" oder "nicht verheiratet" hinausgehen,
- Staatsangehörigkeit, Geburtsdatum, Geburtsort, Geburtsname des Ehegatten und/oder früherer Ehegatten,
- Name, Beruf und Wohnort der Eltern, Angabe des letzten Wohnsitzes verstorbener Eltern,

- Rechtsstatus als Flüchtling oder Vertriebener,
- Nummer des Personalausweises.

Die hin und wieder festgestellte Erhebung der *Personenkennzahl* im Personalbogen habe ich beanstandet und wie folgt bewertet: Die Personenkennzahl darf nur zu Anfragen an die "Gauck-Behörde" verwendet werden. Sie darf nur zu diesem Zweck, ggf. zusammen mit anderen für die Anfrage erforderlichen Daten (z. B. Anschriften der letzten zehn Jahre), *gesondert* erhoben werden und muß dem Gebot des Einigungsvertrages entsprechend zum frühestmöglichen Zeitpunkt - also nach Eingang des Prüfungsergebnisses - gelöscht werden. Ich habe die Behörden aufgefordert, unterbliebene Löschungen nachzuholen.

5.1.6 Einordnung der Unterlagen der Personal- und Fachkommissionen in die Personalakten

Die Datenschutzbeauftragten der neuen Bundesländer vertreten die Auffassung, daß die bei den Personal- und Fachkommissionen entstandenen Unterlagen aus Gründen des Persönlichkeitsschutzes nicht in die Hauptpersonalakte integriert werden sollten. Vielmehr sollten die Unterlagen, ähnlich wie Disziplinarakten, Beihilfeakten oder die Gauck-Unterlagen, getrennt von der Hauptpersonalakte z. B. in einem verschlossenen Umschlag an einer anderen Stelle sicher aufbewahrt werden, weil sie für den normalen Dienstablauf in der personalverwaltenden Stelle nicht erforderlich sind. Durch eine solche Trennung würde verhindert, daß Personen, die zulässigerweise auf Personalakten zugreifen dürfen, Kenntnis vom Inhalt der Kommissionsunterlagen erlangen. Das Personalakteneinsichtsrecht der Betroffenen würde jedenfalls durch diese Handhabung nicht berührt.

Da die Arbeit der Personal- und Fachkommissionen dem Vernehmen nach nahezu abgeschlossen ist, habe ich den Staatsministerien vorgeschlagen, die nachgeordneten Stellen unverzüglich anzuweisen, die Unterlagen der Kommissionen in verschlossenen Umschlägen getrennt von der Hauptpersonalakte an anderer Stelle besonders gesichert aufzubewahren.

5.1.7 MfS/AfNS-Erklärungen

Nach § 6 Abs. 1 Nr. 2 des Sächsischen Beamtengesetzes darf in das Beamtenverhältnis nur berufen werden, wer die Gewähr dafür bietet, daß er jederzeit für die freiheitliche-demokratische Grundordnung im Sinne des Grundgesetzes und der Verfassung des Freistaates Sachsen eintritt. Ein Angestellter im öffentlichen Dienst muß sich nach § 8 Abs. 1 BAT-O durch sein gesamtes Verhalten zur freiheitlichen demokratischen Grundordnung bekennen. Der Einigungsvertrag eröffnet zudem die Möglichkeit einer außerordentlichen Kündigung, wenn ein Beschäftigter für das frühere Ministerium für Staatssicherheit/Amt für Nationale Sicherheit tätig war und deshalb ein Festhalten am Arbeitsverhältnis unzumutbar erscheint (Anlage I Kap. XIX Sachgebiet A Abschnitt III Nr. 1 Abs. 5).

Auf der Grundlage dieser Vorschriften haben Bewerber für den öffentlichen Dienst Erklärungen über eine Mitarbeit für das Ministerium für Staatssicherheit, das Amt für Nationale Sicherheit oder die Ausübung von Mandaten und Funktionen in oder für politische Parteien oder Massenorganisationen der ehemaligen DDR abzugeben. Beschäftigte, die zunächst ohne eine solche Erklärung in den öffentlichen Dienst übernommen worden waren, wurden in einer breit angelegten Fragebogenaktion nachträglich auf ihre Verfassungstreue überprüft.

Im Berichtszeitraum (1.1.1992 - Frühjahr 1993) bildete die datenschutzrechtliche Beurteilung des Inhalts der Fragebogen sowie deren Auswertung und Aufbewahrung einen Schwerpunkt meiner Tätigkeit.

Die mit dem Fragebogen geforderten Angaben habe ich als erforderlich angesehen, damit sich der Dienstherr bzw. Arbeitgeber ein Bild über die Verfassungstreue machen kann. Auch die Erhebung der Personenkennzahl habe ich nicht beanstandet, da sie die Bearbeitung bei der Gauck-Behörde beschleunigt und nur der eindeutigen Identifizierung dient.

Hinsichtlich der Aufbewahrung der Unterlagen, die im Überprüfungsverfahren entstehen, habe ich die Auffassung vertreten, daß das Ergebnis der Entscheidung zur Personalakte zu nehmen ist, die übrigen Unterlagen jedoch gesondert verschlossen aufzubewahren sind, z.B. in einem besonders gekennzeichneten Umschlag zur Personalakte. Sie müssen einer strengen zweckgebundenen Nutzungs- und Zugriffskontrolle unterliegen. Ein Zugriff wird in der Regel nach der Entscheidung über das Grundverhältnis (Einstellung/Übernahme - Nichteinstellung/außerordentliche Kündigung) nicht mehr erforderlich sein, es sei denn, die Entscheidung wird angefochten oder Angaben sind zu überprüfen, weil sich später Hinweise auf - recht häufig vorkommende - Lügen ergeben.

5.1.8 Anrechnung von Beschäftigungszeiten im öffentlichen Dienst der DDR

Zur Feststellung anrechenbarer Beschäftigungszeiten in Bereichen des öffentlichen Dienstes der ehemaligen DDR haben mich eine Reihe von Eingaben und Beschwerden erreicht. Betroffene und Personalräte haben die Rechtmäßigkeit der Ausschluß-tatbestände und die Zulässigkeit bestimmter Fragen angezweifelt. Da ich an der Entwicklung der Fragebogen nicht beteiligt worden war und keine Gelegenheit hatte, in die Verfahrensregelungen Gesichtspunkte des Datenschutzes einzubringen, habe ich mich mit folgenden Hinweisen an das Sächsische Staatsministerium der Finanzen gewandt:

1. Es begegnet bereits erheblichen Zweifeln, ob der *materielle Regelungsinhalt* der Tarifverträge, soweit er sich auf die Anrechenbarkeit früherer Beschäftigungszeiten bei öffentlichen Arbeitgebern der DDR bezieht, in allen Punkten rechtsstaatlicher Überprüfung standhält. Meine verfassungsrechtlichen Zweifel in dieser Hinsicht

richten sich vor allem auf:

- den Versuch, zwischen öffentlichen und privaten Tätigkeiten von DDR-Dienststellen zu differenzieren,
- den undifferenzierten Ausschluß der Anrechenbarkeit jeglicher Tätigkeit als Angehöriger der Grenztruppen der DDR ohne Rücksicht auf die konkrete Dienstfunktion und den bekleideten Rang,
- den unter dem Gesichtspunkt der Normenklarheit unbefriedigenden Ausschlußtatbestand einer Tätigkeitsübertragung auf Grund besonderer persönlicher Systemnähe,
- den Ausschluß systemneutraler Beschäftigungszeiten, die vor einer konkret als nicht anrechenbar qualifizierten Beschäftigungszeit zurückgelegt wurden (Nr. 4 Buchstaben b und c, sowie letzter Satz dieser Nummer, der "Übergangsvorschriften für Zeiten vor dem 1. Januar 1991 zu § 19 BAT-O bzw. § 6 MTArb-O).

Diese Regelungen sind indes unmittelbarer Bestandteil der genannten Änderungs-tarifverträge, denen nach § 1 Tarifvertragsgesetz die Qualität von Rechtsnormen beizumessen ist. Solange diese Bestimmungen rechtlichen Bestand haben, sind sie daher als bereichsspezifische gesetzliche Regelungen anzusehen, hinter denen das allgemeine Datenschutzrecht des Bundes und der Länder zurückzutreten hat (§ 1 Abs. 4 Bundes-datenschutzgesetz; § 2 Abs. 4 SächsDSG).

Angesichts des Vorrangs der Tarifverträge als Spezialrechtsmaterie müssen die in Tarifautonomie vereinbarten Regeln auch von den Verwaltungsbehörden angewendet werden, solange sie nicht durch verfassungsgerichtliche Entscheidung aufgehoben werden.

2. Datenschutzrechtlich überprüfbar bleiben aber die Hinweise und Erläuterungen, die in der Bekanntmachung des Bundesministers des Innern von 18.12.1991 (GMBl. 1992, S. 90) enthalten sind oder die als "Hinweise zum Ausfüllen des Antrages" von anderer, als Verfasser nicht erkennbarer Stelle gegeben worden sind. Das gleiche gilt für die Erläuterungen, die in dem "Merkblatt zum Vollzug der Tarifverträge über die Anerkennung von Beschäftigungszeiten" gemacht werden, das gleichfalls weder den Verfasser noch das Datum der Herausgabe ausweist.

In den "Hinweisen zum Ausfüllen des Antrages" wird angemerkt, daß alle im Antrag auf Anerkennung von Beschäftigungszeiten gemachten Angaben vom Beschäftigten "zu beweisen" sind. Dieser Hinweis findet in den Tarifverträgen keine Stütze; es widerspricht auch den allgemeinen Beweislastregeln, denen zufolge bei Ausschluß- oder Ausnahmeregeln derjenige beweislastet ist, der sich auf den Ausnahme- oder Ausschlußtatbestand beruft.

Auch aus § 21 bzw. § 8 der Tarifverträge läßt sich die Beweislast des Betroffenen nicht

ableiten. Danach hat der Angestellte oder Arbeiter zwar innerhalb einer bestimmten Ausschlußfrist die Nachweise seiner früheren Beschäftigungszeiten vorzulegen. Diese Nachweispflicht bezieht sich aber ersichtlich nur auf die faktische Darlegung der früheren Beschäftigungsverhältnisse und ihrer Zeitdauer, nicht aber auf die Frage, ob die wahrgenommenen Funktionen zu den von der Anrechenbarkeit ausgeschlossenen oder nicht ausgeschlossenen Tätigkeiten i. S. der Nr. 4 Buchst. a und b der "Übergangsvorschriften" zu § 19 bzw. § 6 der Tarifverträge gehörten. Dieser Hinweis trägt auch nicht dem Gesichtspunkt Rechnung, daß der Betroffene in Fällen der vermuteten Funktionsbetrauung auf Grund besonderer persönlicher Systemnähe diese Vermutung bereits durch das glaubhafte Vorbringen von Indizien für einen anderen Geschehensablauf entkräften kann, nicht aber den vollen Beweis des Gegenteils führen muß.

Das Merkblatt und das Fragebogenmuster lassen nicht mit der gebotenen Deutlichkeit für den Betroffenen erkennen, inwieweit die geforderten Daten zur Entscheidung über die Anrechenbarkeit früherer Beschäftigungszeiten relevant sind und wie die zuständige Verwaltung in den verschiedenen denkbaren Fallkonstellationen einer Funktionsbetrauung auf Grund besonderer Systemnähe entscheiden wird. Die Formulierung der Spalte 8 des Fragebogens und die insoweit gegebenen Ausfüllhinweise machen es für den Betroffenen nicht nachvollziehbar, welche Kriterien der Entscheidung über die Anrechenbarkeit der Zeiten konkret zugrunde gelegt werden; diese Formulierungen werden insoweit dem Grundsatz der Zweckbindung der erhobenen Daten für einen klar ausgewiesenen Verwaltungsvollzug nicht gerecht. Es würde die Transparenz der Zielrichtung der Fragen für den Betroffenen bereits deutlich verbessern, wenn die Texte der Änderungstarifverträge, zumindest die in ihnen enthaltenen "Übergangsvorschriften für Zeiten vor dem 1. Januar 1991", den Fragebögen beigefügt würden.

Soweit den Betroffenen in dem Fragebogen eine lückenlose Darstellung des beruflichen Werdeganges einschließlich der Ausbildung, beginnend mit dem 14. Lebensjahr, aufgegeben wird, geht die Fragestellung über den Datenerhebungszweck hinaus, wenn der Betroffene für eine derart weit zurückreichende Zeitspanne eine Anrechnung früherer Beschäftigungs- oder Ausbildungszeiten gar nicht begehrt. Hier bedarf es daher eines klarstellenden Hinweises, daß die " lückenlose" Darstellung des Werdeganges nur für diejenigen Zeiten erforderlich ist, für die der Betroffene eine Anrechnung geltend macht.

Die von mir angesprochenen Probleme wurden in einem Gespräch mit dem Sächsischen Staatsministerium der Finanzen erörtert. Ich gehe davon aus, daß das Problemfeld uns noch länger beschäftigt.

5.1.9 Anhörungsrechte Betroffener

Im Berichtszeitraum habe ich mehrfach festgestellt, daß Behörden vor einer den Einzelnen belastenden Maßnahme nur unzureichend das gesetzlich vorgeschriebene Recht auf Anhörung gewährt haben. Ich habe aus datenschutzrechtlicher Sicht hierzu Stellung genommen, weil eine fehlerhafte oder unterbliebene Anhörung stets in das informationelle Selbstbestimmungsrecht des Einzelnen eingreift. Hiernach hat jedermann das Recht zu wissen, welche Daten über ihn bei welcher öffentlicher Stelle gespeichert sind und wie diese genutzt werden sollen.
Anhörungsrechte finden sich in unterschiedlichen Rechtsgebieten:
Nach § 119 Sächsisches Beamtengesetz (SächsBG) ist der Beamte zu Beschwerden, Behauptungen und Bewertungen, die für ihn ungünstig sind oder für ihn nachteilig werden können, vor deren Aufnahme in die Personalakte zu hören. Eine ähnliche Vorschrift enthält der Bundesangestelltentarif (BAT) in § 13 Abs. 2 für Angestellte im öffentlichen Dienst.
Ein erweitertes Anhörungsrecht enthält das Sächsische Hochschulerneuerungsgesetz (SHEG) im Zusammenhang mit der Frage der Abberufung von Professoren oder der Kündigung von Mitarbeitern der Hochschulen. Gemäß § 78 Abs. 2 S. 1 SHEG hat die Personalkommission der jeweiligen Hochschule vor einer Entscheidung den Betroffenen rechtliches Gehör, insbesondere Gelegenheit zur Stellungnahme zu allen von ihr herangezogenen Unterlagen zu gewähren. Hat die Personalkommission entschieden, ob sie dem Staatsministerium die Abberufung von Professoren oder die Kündigung von Mitarbeitern empfiehlt, fordert sie gemäß § 78 Abs. 3 S. 3 SHEG den Betroffenen erneut zur Stellungnahme auf. Es ist also in dem Verfahren sogar eine "doppelte Anhörung" vorgesehen.
Das allgemeine Anhörungsrecht im Verwaltungsverfahren ist in § 28 Verwaltungsverfahrensgesetz (VwVfG) geregelt, wonach den Beteiligten vor Erlaß eines belastenden Verwaltungsakts die Gelegenheit zur Äußerung eingeräumt werden muß.
Das Recht zur Anhörung fußt auf dem in Art. 1 Grundgesetz festgelegten Gebot des Schutzes der Menschenwürde, wonach der Einzelne nicht lediglich das Objekt einer Entscheidung sein kann. Durch die Anhörung soll der Betroffene vor Überraschungsentscheidungen geschützt werden. Darüber hinaus ist die Anhörung regelmäßig notwendige Voraussetzung für eine sachlich richtige Maßnahme, da sie der Aufklärung des Sachverhalts dient. Zur Gewährleistung des Anhörungsrechts hat daher eine Behörde dem Einzelnen vor einer abschließenden Entscheidung die nach ihrer Auffassung erheblichen Tatsachen mitzuteilen, soweit diese nicht bereits bekannt sind, und zur Stellungnahme aufzufordern. Hierzu kann die Gewährung von Akteneinsicht mit einem entsprechenden Hinweis zur Äußerung ausreichen. Ausnahmsweise kann aber auch die Überlassung einer Akte geboten sein, wenn ein besonders sorgfältiges Aktenstudium notwendig ist. Bei rechtlich komplizierten Sachverhalten sollte die Behörde außerdem die zugrunde gelegte Rechtsauffassung mitteilen.
Die Einholung der Äußerung des Betroffenen muß so rechtzeitig erfolgen, daß diesem genügend Zeit bleibt, sich mit dem Verfahrensstoff vertraut zu machen und eine Stellungnahme gegebenenfalls durch einen Bevollmächtigten vorzubereiten. Werden in

das Verfahren neue Tatsachen eingebracht, zu denen der Beteiligte noch nicht gehört worden ist, muß eine erneute Anhörung stattfinden.

Nach meinen Feststellungen sind in der Vergangenheit behördliche Entscheidungen ergangen, ohne daß mit den Betroffenen der zugrunde liegende Sachverhalt ausreichend erörtert worden ist. So sind ohne ausreichende Anhörung Kündigungen wegen einer Tätigkeit für das MfS/AfNS ausgesprochen worden, weil auf Grund einer solchen Tätigkeit davon ausgegangen wurde, daß der Beschäftigte keine Gewähr für die Verfassungstreue bietet.
Das Bundesarbeitsgericht hat entschieden, daß Unterlagen der Gauck-Behörde nur dann für eine Kündigung herangezogen werden dürfen, wenn der Betroffene sich zuvor mit diesen Akten vertraut machen konnte.

5.1.10 Personalunterlagen für das Landesamt für Finanzen

Ein Oberschulamt hat sich dagegen gewandt, daß das Landesamt für Finanzen (LfF) im Fall einer Kündigung wegen der Beendigung der Bezügezahlungen die Kündigungsunterlagen verlangt, die bei außerordentlichen Kündigungen nach § 54 BAT-O umfangreiche Begründungen zur politischen Vergangenheit des Gekündigten enthalten.

Das LfF begründete dies damit, daß es zu prüfen habe, ob anteilige Sonderzuwendungen oder bei Bedarfskündigungen die Zahlung von Abfindungen in Betracht kommen.

Ich habe gegenüber dem Staatsministerium für Finanzen (SMF) meine Auffassung dargelegt, daß es nicht Aufgabe der bezügezahlenden Stelle sei, die finanziellen Auswirkungen von Kündigungen rechtlich zu beurteilen und daß zur Einstellung von Zahlungen Originalunterlagen oder Kopien aus Personalakten nicht erforderlich seien. Als datenschutzgerechte Lösung habe ich Mitteilungen vorgeschlagen, die nur die für das LfF notwendigen Daten enthalten. Das LfF verzichtet seitdem auf die Übermittlung der Kündigungsgründe. Im Hinblick auf ein landesweit einheitliches Verfahren erarbeitet das SMF derzeit ein Gesamtkonzept über die Zuständigkeiten des LfF, das auch regeln soll, welche Daten die Personalstellen mitzuteilen haben. Die weitere Entwicklung werde ich beobachten.

5.1.11 Beteiligung des Sächsischen Datenschutzbeauftragten bei der automatisierten Verarbeitung von Personaldaten

Die automatisierte Verarbeitung von Daten der Beschäftigten darf nach § 31 Abs. 7 SächsDSG nur *im Benehmen mit dem Datenschutzbeauftragten* eingeführt, angewendet, geändert oder erweitert werden. Diese Bestimmung wird weitgehend nicht beachtet. Ich habe deshalb in meiner Bekanntmachung zu § 31 Abs. 7 SächsDSG vom 10. Dezember

1992 (s. Nr. 16.1.3) die öffentlichen Stellen aufgefordert, bisher nicht gemeldete Verfahren anzuzeigen.

Wichtig ist dabei nicht nur, für meine Prüfungstätigkeit einen Überblick über die bereits eingesetzten Verfahren zu erhalten, sondern auch die Personalvertretungen durch meine Stellungnahmen in die Lage zu versetzen, die Verfahren im Hinblick auf ihre Auswirkungen auf die Bediensteten beurteilen zu können. Denn § 31 Abs. 7 SächsDSG verpflichtet die Behördenleitung zur Weitergabe der Stellungnahme an die zuständige Personalvertretung.

In der Bekanntmachung sind alle Angaben aufgeführt, die ich benötige, um die Rechtmäßigkeit und Erforderlichkeit eines Verfahrens beurteilen zu können.

5.1.12 Elektronische Zeiterfassung

5.1.12.1
Stechuhren oder personelle Aufzeichnungen über geleistete Arbeitszeiten werden zunehmend durch elektronische Zeiterfassungssysteme ersetzt. Im Berichtszeitraum hatte ich unterschiedliche Systeme und Verfahren zu beurteilen. Meinen Feststellungen zufolge wurden die automatisierten Zeiterfassungsverfahren als in Hard- und Software eigenständige, mit anderen EDV-Systemen nicht verbundene Anlage installiert. Die Zeit wird für jeden Mitarbeiter über seine Code-Karte und das Buchungsterminal erfaßt, das beim Betreten oder Verlassen des Gebäudes zu betätigen ist. Mehr- oder Fehlzeiten werden dem Mitarbeiter über eine Auskunftstaste in Verbindung mit seiner Code-Karte angezeigt. Gesonderte Eingabeterminals dienen der Einrichtung, Änderung, Löschung und Abfrage der Zeitwertkonten.

Fehlgründe, die sich nicht arbeitszeitmindernd auswirken, sog. erlaubte Fehlzeiten (z.B. Urlaub, Krankheit, Dienstreisen), werden nicht vom Mitarbeiter, sondern entweder direkt in der EDV-Stelle von dem mit der Betreuung des Zeiterfassungssystems Beauftragten oder von der Personalstelle den Zeitkonten zugebucht.

In allen Fällen war beabsichtigt, das System später auch für die Zugangskontrolle einzusetzen. Zwei Beispiele sollen die datenschutzrechtliche Problematik elektronischer Zeiterfassungssystem aufzeigen:

5.1.12.2
Das System in einem Landratsamt eröffnet über die reine Zeiterfassung hinaus eine Reihe von Möglichkeiten, Listen und Auswertungen bezogen auf einzelne Mitarbeiter oder Mitarbeitergruppen unter den verschiedensten Gesichtspunkten zu erstellen. So können aus den Zeitwertdaten Abwesenheits-, Urlaubs- und Krankheitslisten erstellt werden sowie Listen aller Mitarbeiter mit bestimmten Mehr- oder Fehlzeiten. Möglich ist auch die Speicherung sensibler personenbezogener Merkmale (Personenstand, Geschlecht, Geburtstag, Schwerbehinderteneigenschaft, Status als Beamter oder

Angestellter) in nicht vordefinierten Datenfeldern, um sie für spätere Auswertungen nutzen zu können.

Ich habe es deshalb begrüßt, daß nur die für die Arbeitszeiterfassung erforderlichen Daten gespeichert werden: Ausweisnummer der Code-Karte, Name und Vorname des Karteninhabers, Abteilung und dienstliche Telefonnummer. Mithin unterbleibt die Nutzung einiger Möglichkeiten.

Nach § 31 Abs. 5 SächsDSG dürfen Daten, die für eine (zulässige) Verhaltens- oder Leistungskontrolle erhoben werden, nur zu diesem Zweck genutzt werden. Ich habe deshalb keine Bedenken gegen Auswertungen erhoben, die der Durchführung der Dienstaufsicht dienen oder zu Kontrollzwecken (z. B. Revision, Datensicherheit) angefertigt werden. Als positiv habe ich es gewertet, daß keine turnusmäßigen Übersichten über geleistete Arbeitszeiten, Mehr- oder Fehlzeiten erstellt werden, und zwar weder für die Vorgesetzten noch für die Mitarbeiter. Eine regelmäßige Auswertung gespeicherter Zeitwertdaten erfolgt nur zur Erfassung von "Kernzeitverletzern". Bereits nach drei Monaten werden die Zeitwertdaten gelöscht.

Die Erfassung der erlaubten Fehlzeiten erfolgt in der EDV-Stelle durch den mit der Betreuung des Zeiterfassungssystems Beauftragten. Zu diesem Zweck werfen die Mitarbeiter Zettel mit den betreffenden Angaben in einen dafür vorgesehenen Briefkasten. Aus datenschutzrechtlicher Sicht ist dieses Verfahren akzeptabel.

Die systemseitig vorgesehenen Maßnahmen zur Gewährleistung der Datensicherheit sind ausreichend, die Anforderungen an den Paßwortschutz jedoch mangelhaft, so daß ich entsprechende Empfehlungen ausgesprochen habe; vgl. dazu unten Nr. 16.3.4.

Zwar hatte die Personalvertretung der Einführung der elektronischen Zeiterfassung zugestimmt, eine Dienstvereinbarung war jedoch nicht getroffen worden. Ich habe ihr deshalb für den Umgang mit Personaldaten im innerdienstlichen Bereich im Hinblick auf § 80 Abs. 3 Nr. 16 des Sächsischen Personalvertretungsgesetzes den Abschluß einer Dienstvereinbarung empfohlen, in der folgendes geregelt werden sollte:

- Gegenstand und Geltungsbereich der Dienstvereinbarung,
- Zweck der automatisierten Personaldatenverarbeitung, Zweckbindung der Daten,
- Datenspeicherung (Art und Umfang, Zulässigkeit/Nichtzulässigkeit der Verknüpfung mit andern EDV-Verfahren, Auswertungsrahmen),
- Rechte der Beschäftigten (insbesondere Auskunftsrecht nach § 31 Abs. 3 i. V. m. § 17 SächsDSG),
- Verbot der Auswertung von Archivdateien zur Erstellung von Persönlichkeitsprofilen der Beschäftigten,
- Zugriffsberechtigungen für verfahrensbeteiligte Sachbearbeiter und Vorgesetzte im Rahmen ihrer sachlichen und personellen Zuständigkeit,
- Beteiligung der Personalvertretung bei der Weiterentwicklung von Verfahren zur automatisierten Personaldatenverarbeitung,

- Inkrafttreten und Laufzeit der Dienstvereinbarung.

Ich habe darauf hingewiesen, daß ich rechtzeitig vor dem Einsatz des Systems für Zwecke der Zugangskontrolle zu unterrichten bin.

5.1.12.3
Auch das Sächsische Staatsministerium der Finanzen (SMF) hat mich vor Einführung eines elektronischen Zeiterfassungssystems um eine datenschutzrechtliche Beurteilung gebeten und mich davon in Kenntnis gesetzt, daß auch andere Ministerien beabsichtigen, dieses System nach Abschluß einer Testphase im SMF einzuführen.

In meiner Stellungnahme bin ich nicht nur auf die datenschutzrechtlichen Gesichtspunkte eingegangen, sondern habe grundsätzlich angemerkt, daß ich die elektronische Zeiterfassung in *obersten Dienstbehörden* für unangemessen halte.

Von Ausnahmen abgesehen kann jeder Referatsleiter übersehen, wer die Dienstzeiten nicht einhält. Eine "Mauerermentalität" wäre einer Ministerialarbeit eher abträglich, sie verstärkt möglicherweise die Kritik an der Ministerialzulage. Der vorgesehene bürokratische und finanzielle Aufwand der Anlage ist aus meiner Sicht unerträglich.
Mithin ist der Eingriff in das Persönlichkeitsrecht der Mitarbeiter nicht erforderlich; die Datenerfassung ist nicht notwendig. Ein Anspruch der Belegschaft oder der Personalvertretung auf Einführung der elektronischen Zeiterfassung besteht nicht.

Abgesehen von meiner grundsätzlichen Ablehnung einer elektronischen Zeiterfassung in Ministerien habe ich begrüßt, daß die mit dem Personalrat getroffene Dienstvereinbarung Regelungen enthält, die die Anforderungen an den Datenschutz erfüllen: So sind die im Zusammenhang mit der Zeiterfassung zu speichernden Daten festgelegt und dem datenschutzrechtlichen Gebot der Erforderlichkeit entsprechend auf den notwendigen Umfang begrenzt worden. Der Zugriff auf die Zeitwertdaten ist nur den verfahrensbeteiligten Sachbearbeitern und ihren Vorgesetzten gestattet.

Für Zwecke der Dienstaufsicht darf auch der Vorgesetzte eines Beschäftigten Daten aus den Aufzeichnungen des Zeiterfassungssystems erhalten. Als positiv habe ich die Pflicht zur vorherigen Information des Beschäftigten gewertet. Da zum Zeitpunkt meiner Stellungnahme noch offen war, wie das Auskunftsverfahren für die Praxis ausgestaltet werden soll, habe ich dargelegt, daß eine nur *mündliche* Anforderung des Vorgesetzten und eine *mündliche* Information des Beschäftigten keine datenschutzgerechte Lösung darstellen. Vielmehr sollte die Auskunftserteilung an eine *schriftliche* Anforderung geknüpft werden und die Auskunftserteilung davon abhängig sein, daß der Beschäftigte seine vorherige Information durch Unterschrift oder Namenszeichen auf der Anforderung bestätigt hat. Klärungsbedürftig ist allerdings, wer die Berechtigung des Anfragenden zu prüfen, also festzustellen hat, ob der Anfragende Vorgesetzter des Betroffenen ist.

Die Dienstvereinbarung führt die zulässigen Auswertungen und Ausdrucke abschließend auf. Programmtechnische Maßnahmen gewährleisten, daß unzulässige Ausdrucke (Auflistung von Kommt/Geht-Zeiten eines Beschäftigten während der Kernarbeitszeit, Auflistung von "Kernzeitverletzern") nicht erstellt werden können; aus datenschutzrechtlicher Sicht eine brauchbare Lösung.

Allerdings waren Aufbewahrungsfristen für einige Ausdrucke und Löschungsfristen für die gespeicherten Zeitwertdaten bzw. der betreffenden Datenträger nicht bestimmt worden. Der Zeitraum sollte sich an den Fristen für Geschäftsprüfungen sowie an der Verfolgungsverjährung für geringere Dienstvergehen orientieren. Ergänzend habe ich auf § 19 Abs. 1 Nr. 2 SächsDSG hingewiesen, wonach personenbezogene Daten in Dateien zu löschen sind, wenn ihre Kenntnis zur Aufgabenerfüllung der speichernden Stelle nicht mehr erforderlich ist.

Für die Bedienung des Systems soll ein sog. "Gleitzeitbeauftragter" berufen werden. Zur Erfassung von Fehlzeiten, die sich nicht arbeitszeitmindernd auswirken dürfen, leitet ihm die Personalstelle Urlaubsanträge, Krankmeldungen, Dienstreiseanträge usw. zu. Selbstverständlich unterliegt der Gleitzeitbeauftragte besonderen Verschwiegenheitspflichten.

5.1.13 Mißbrauch von Personaldaten

Einer Beanstandung der Stadtverwaltung Dresden lag folgender Sachverhalt zugrunde:
Der Leiter einer Heimeinrichtung der Stadtverwaltung Dresden fand einen handschriftlichen anonymen Brief, in dem seine Überprüfung durch die Gauck-Behörde gefordert wurde. Diese Forderung entsprach der Rechtslage. Dennoch fertigte der Leiter, ohne Wissen und Einwilligung der Betroffenen, Kopien von Handschriften aus den Personalakten von vier ihm als Briefschreiber verdächtig erscheinenden Mitarbeitern. Er übergab diese Kopien einer Dresdner Privatdetektei, die die Unterlagen vom einem kriminaltechnischen Institut auf Identität mit dem Schriftbild des anonymen Briefes überprüfen ließ. Nach Eingang des graphologischen Gutachtens beschuldigte er einen der vier verdächtigten Mitarbeiter, der Urheber des Schreibens gewesen zu sein, ohne daß er dies beweisen konnte. Die Kosten des Auftrags, ca. 1500 DM, wurden aus Mitteln der Stadt finanziert. Die Nutzung und Übermittlung der Daten aus den Personalakten waren weder zur Erfüllung der Personalaufgaben der Stadtverwaltung erforderlich, noch wurden die Daten für die Zwecke genutzt, für die sie erhoben worden waren.

Ich sehe einen Verantwortungs- und Organisationsmangel bereits darin, daß ein Heimleiter Personalakten verwaltet. Diese gehören in die Obhut des zentral zuständigen Personalamtes der Stadt.

Eine Personalakte wird zu personalrechtlichen Bearbeitungszwecken oder zu Zwecken der Personalwirtschaft geführt. Der innerbehördliche Zugriff auf eine Personalakte

ist nur erlaubt, soweit er für diese Zwecke erforderlich ist; private Verfolgungsinteressen rechtfertigen einen Zugriff keinesfalls.
Das Verhalten des Heimleiters, welches sich die Behörde zurechnen lassen muß, war auch nicht im Interesse des Hausfriedens geboten. Eine kurzfristige und geringfügige Schädigung seines Rufes im Hause mußte der Heimleiter hinnehmen, zumal er selbst den anonymen Brief im Heim "an die große Glocke hängte" und die im Schreiben enthaltene Forderung der Rechtslage entsprach.

Schließlich war die Weiterleitung des Inhalts eines Teils der Personalakten an die Privatdetektei zweckwidrig. Die Weiterleitung läßt sich nicht dadurch rechtfertigen, daß die Detektei privatrechtlich zur Geheimhaltung verpflichtet war. Ein Verstoß gegen dienstliche Geheimhaltungspflichten, die sich hier aus der Fürsorgepflicht des Arbeitgebers ergeben, liegt auch dann vor, wenn der Adressat von Mitteilungen selbst hierüber schweigen soll.

Wider Erwarten hat die Verwaltung der Stadt Dresden meine entsprechenden Hinweise nicht entgegengenommen, sondern allerlei Ausflüchte gesucht. Als besonders gravierend habe ich den Hinweis empfunden, daß die Aktenverwaltung eine Aufgabe der kommunalen Selbstverwaltung darstelle, über deren Art die Kommune bestimme. Aus dieser Anmerkung ist zu folgern, daß die Stadtverwaltung Dresden den Bereich der kommunalen Selbstverwaltung für einen rechtsfreien Raum hält, der folgerichtig auch nicht meiner Kontrolle unterläge. Deshalb hat das Staatsministerium des Innern zwischenzeitlich das Regierungspräsidium Dresden gebeten, die Stadt Dresden in geeigneter Weise darauf hinzuweisen, daß die kommunale Selbstverwaltung *nur im Rahmen der Gesetze* gewährleistet sei. Zu diesen Gesetzen, die die kommunale Selbstverwaltung insoweit einschränken, gehöre auch das Sächsische Datenschutzgesetz. Der Sächsische Datenschutzbeauftragte könne daher ohne weiteres auch gegenüber der Stadt Dresden von seinen gesetzlichen Befugnissen Gebrauch machen. In welcher Form dieser Hinweis weitergegeben wurde, ist mir nicht bekannt.

Die Stadt Dresden hat angegeben, die Personalakten seien "soweit erforderlich" zentriert worden. Konkrete Maßnahmen hat sie jedoch nicht mitgeteilt. Ich werde in Kürze eine entsprechende Kontrolle durchführen.

Die Stadt Dresden hat offenbar besondere Gründe, weshalb sie den verschiedenen Aufforderungen mitzuteilen, ob die vom Heimleiter zu Unrecht verwendeten Mittel zurückbezahlt sind, bisher nicht nachgekommen ist.

Unverständlich ist mir die sinngemäß geäußerte Auffassung der Stadt Dresden, für sie bestünde kein Anlaß, sich bei den zu Unrecht verdächtigten Mitarbeitern zu entschuldigen. "Eine solche Entschuldigung obliegt allein demjenigen, der fehlerhaft gehandelt hat, nicht also der Stadtverwaltung als Behörde, der dies nicht vorwerfbar ist", meint die Stadtverwaltung Dresden. Aus dieser Auffassung ist zu entnehmen, daß die Stadt Dresden sich nicht verpflichtet fühlt, für die Handlungen ihrer Funktionsträger in Ausübung des Amtes einzutreten.

Von der Möglichkeit, gemäß § 26 Abs. 2 Sächsisches Datenschutzgesetz von einer Beanstandung abzusehen, habe ich in diesem Fall keinen Gebrauch gemacht. Dies setzt voraus, daß die öffentliche Stelle, bei der die Verstöße gegen datenschutzrechtliche Bestimmungen zu verzeichnen sind, auch bereit ist, die eigenen Fehler einzusehen und konkrete Maßnahmen zu treffen, damit sich derartige Vorgänge nicht wiederholen. An dieser Bereitschaft fehlt es der Stadtverwaltung Dresden.

5.2 Personalvertretung

5.2.1 Personalvertretungsgesetz

Das Sächsische Personalvertretungsgesetz vom 21. Januar 1993 (GVBl. S. 29) räumt den Personalvertretungen weitgehende Rechte ein, um den Persönlichkeitsschutz von Beschäftigten im öffentlichen Dienst sicherzustellen.

Es handelt sich um datenschutzrechtlich bedeutsame Regelungen zur Mitbestimmung bei der Einführung und Anwendung technischer Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen (z. B. Arbeitszeiterfassung, Aufzeichnung von Telefonaten). Vorschriften zur rechtzeitigen und umfassenden Unterrichtung der Personalvertretung sollen garantieren, daß die Mitbestimmung sinnvoll ausgeübt werden kann. Die Aufgabe des Personalrats, sich im Rahmen des Mitbestimmungsrechts ein Urteil über die Hard- und Software zu bilden, unterstütze ich im Rahmen des § 31 Abs. 7 SächsDSG (vgl. unten Nr. 16.1.3).

Von datenschutzrechtlicher Bedeutung ist außerdem, daß die Einsichtnahme in die Personalakte durch Mitglieder der Personalvertretung in jedem Einzelfall von der Einwilligung des Beschäftigten abhängig ist und daß dieser bestimmen kann, welche Personalratsmitglieder die Akte einsehen dürfen.

Personen, die Aufgaben oder Befugnisse nach dem Personalvertretungsgesetz wahrnehmen oder wahrgenommen haben, sind über die ihnen dabei bekanntgewordenen Angelegenheiten und Tatsachen zu Stillschweigen verpflichtet. Die Sitzungen des Personalrats sind nicht öffentlich.

5.2.2 Nichtöffentlichkeit von Personalratssitzungen

Ein Personalrat hat die Niederschrift über eine Personalratssitzung an einen Landtagsabgeordneten weitergegeben. Sie sollte diesem als konkrete Grundlage für eine Anfrage an die Staatsregierung dienen. Die vollständige Niederschrift, die auch personenbezogene Daten Unbeteiligter enthielt, wurde später als Anlage zu einer Landtagsdrucksache vervielfältigt.

Ich habe den Personalrat auf die Vertraulichkeit der Beratungsgegenstände und das Gebot der Nichtöffentlichkeit von Personalratssitzungen hingewiesen.

5.2.3 Beteiligung der Schwerbehindertenvertretung

Eine Anfrage veranlaßte mich zu prüfen, ob es zulässig sei, der Schwerbehindertenvertretung Bewerbungsunterlagen Behinderter und Nichtbehinderter vorzulegen, damit die Qualifikation Nichtbehinderter im Vergleich zu Schwerbehinderten beurteilt werden könne.

Ich habe dazu folgende Auffassung vertreten:
Nach § 14 Abs. 1 Satz 2 Schwerbehindertengesetz (SchwBG) sind Bewerbungen von Schwerbehinderten mit der Schwerbehindertenvertretung lediglich zu *erörtern*. Aus diesem Wortlaut läßt sich für die Schwerbehindertenvertretung nicht das Recht ableiten, an den Vorstellungsgesprächen aller Bewerber teilzunehmen bzw. deren Bewerbungsunterlagen einzusehen. Das gilt auch dann, wenn sich unter den Bewerbern mindestens ein Schwerbehinderter befindet.

Ein solches Verfahren würde sowohl gegen das informationelle Selbstbestimmungsrecht behinderter als auch nichtbehinderter Bewerber verstoßen. Denn die Regelung in § 14 Abs. 1 letzter Satz SchwBG, daß der Schwerbehinderte die Erörterung seiner Bewerbung mit der Schwerbehindertenvertretung ablehnen kann, verbietet geradezu, Bewerbungsunterlagen ohne Einwilligung der Betroffenen der Schwerbehindertenvertretung vorzulegen.

5.3 Meldewesen

5.3.1 Rechtliche Entwicklung

Nach dem Einigungsvertrag galt vorübergehend für das Einwohnermeldewesen das Melderechtsrahmengesetz. Der Gesetzgeber war also aufgerufen, ein eigenes Sächsisches Meldegesetz zu erlassen, um die allenthalben feststellbare Rechtsunsicherheit zu beseitigen.

Vom Staatsministerium des Innern wurde ich dankenswerterweise frühzeitig in die Verhandlungen zum Gesetzentwurf einbezogen. Zu dem inzwischen sich im parlamentarischen Verfahren befindenden Entwurf eines Sächsischen Meldegesetzes habe ich eine datenschutzrechtliche Stellungnahme abgegeben.
Insbesondere habe ich mich kritisch zur Frage der Zulässigkeit von Auftragsdatenverarbeitung durch private Rechenzentren geäußert. Die Sensibilität der Meldedaten (u. a. Steuerdaten, Adoptivdaten, nichteheliche Kinder, Transsexuelle, Paßversagungen, Wahlausschlüsse, Patienten- und Behindertendaten, JVA-Insassen) gebietet, daß die Verarbeitung tunlichst bei der öffentlichen Hand verbleibt.
Ich habe auch eine Regelung angeregt, die eine denkbare Beeinträchtigung schutzwürdiger Interessen der Betroffenen bei der Herausgabe von Adreßbüchern ausschließt (z. B. Heraussortieren der Insassen von Justizvollzugsanstalten oder von Personen, die in einem Krankenhaus, Pflegeheim oder einer sonstigen Einrichtung gemeldet sind, die der Betreuung pflegebedürftiger oder behinderter Menschen, der

Rehabilitation oder der Heimerziehung dient oder Sortieren nach Geschlecht oder mutmaßlichem Familienstand).

Ebenso habe ich angeregt, im Melderegister eine Kennzeichnung des Personenkreises vorzusehen, der nach § 41 Wehrpflichtgesetz zwei Jahre von der Wehrerfassung befreit ist (z. B. Aussiedler). Ohne eine solche Kennzeichnung würden die Betroffenen womöglich rechtswidrig wehrerfaßt und eingezogen.

Erfreulicherweise stand der Gesetzgeber meinen Änderungs- und Ergänzungsvorschlägen aufgeschlossen gegenüber.

Zu begrüßen ist, daß der Meldegesetz-Entwurf in einer ganzen Reihe von Bestimmungen bereichsspezifisch das informationelle Selbstbestimmungsrecht der Betroffenen berücksichtigt. Hervorzuheben sind die abschließende Aufzählung der zu speichernden Meldedaten, der Grundsatz der Zweckbindung, das Meldegeheimnis sowie die Schutzrechte des Betroffenen (Auskunftsanspruch, Berichtigungsanspruch, Löschungsanspruch, Anhörung und Benachrichtigung des Betroffenen bei erweiterten Melderegisterauskünften, Auskunftssperren, Widerspruchsrechte).

5.3.2 Gruppenauskünfte, Jubiläumsdaten, Einwohnerdaten im Adreßbuch

Das künftige Meldegesetz sieht vor, daß die Meldebehörde unter gewissen Voraussetzungen den politischen Parteien und Wählergruppen Wähleranschriften zum Zwecke der Wahlwerbung übermitteln darf. Außerdem dürfen Alters- und Ehejubiläen veröffentlicht oder an Presse, Rundfunk oder andere Medien zum Zwecke der Veröffentlichung übermittelt werden. Auch ist die Veröffentlichung von Einwohnderdaten in Adreßbüchern vorgesehen. Da nicht jeder Betroffene dies wünscht, wird ihm das Recht zugestanden, ohne Nennung von Gründen der Veröffentlichung bzw. der Weitergabe seiner Daten zu den genannten Zwecken zu *widersprechen*. Die Widersprüche können der zuständigen Meldebehörde mitgeteilt werden.

5.3.3 Die Übermittlung von Meldedaten an die Gebühreneinzugszentrale der Rundfunkanstalten

Die Sächsische Staatskanzlei bat mich, zu einem Rechtsgutachten, in dem die Rechtmäßigkeit und Erforderlichkeit einer regelmäßigen Meldedatenübermittlung an die Gebühreneinzugszentrale der Rundfunkanstalten (GEZ) untersucht wird, Stellung zu nehmen.

Da mit entsprechenden Übermittlungswünschen der GEZ auch in Sachsen zu rechnen ist, habe ich der Staatskanzlei und dem Staatsministerium des Innern vorsorglich meine Bedenken gegen eine regelmäßige Übermittlung der Daten aller volljährigen Einwohner an die GEZ mitgeteilt. Nach § 29 Abs. 5 des Sächsischen Meldegesetz-Entwurfs sind regelmäßige Datenübermittlungen nur zulässig, soweit dies durch

Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zwecks der Übermittlungen, der Empfänger und der zu übermittelnden Daten bestimmt ist. Bislang gibt es m. W. entsprechende (aber umstrittene) Rechtsgrundlagen, die Datenübermittlung an die GEZ erlauben, nur in den Meldedatenübermittlungsverordnungen Hessens und Nordrhein-Westfalens.

Vorbehaltlich der entsprechenden Ermächtigungsnorm im Sächsischen Meldegesetz vertrete ich die Auffassung, daß eine regelmäßige Datenübermittlung an eine andere öffentliche Stelle nur unter Beachtung des Erforderlichkeitsgrundsatzes zur rechtmäßigen Aufgabenerfüllung erfolgen darf. Außerdem darf durch die Datenübermittlung das informationelle Selbstbestimmungsrecht der Betroffenen nicht im Kern dieses Grundrechts oder unverhältnismäßig, gemessen am öffentlichen Interesse am Eingriff, beeinträchtigt werden. Erforderlich ist eine solche Datenübermittlung m. E. dann, wenn sie zur Erreichung des Zwecks der Aufgabe objektiv geeignet ist und im Verhältnis zum angestrebten Zweck als angemessen erscheint. Als Aufgabe der Rundfunkanstalten und der GEZ ist in diesem Sinne der Einzug der Rundfunkgebühren nach dem Rundfunkgebührenstaatsvertrag anzusehen.

Eine regelmäßige Übermittlung personenbezogener Meldedaten aller volljährigen Einwohner dient zwar möglicherweise der GEZ dazu, vorhandene Datenbestände zu aktualisieren; eine Notwendigkeit oder auch nur eine besondere Eignung für den Einzug der Rundfunkgebühren anzunehmen, ist aber zumindest problematisch. Die Meldedaten sind nämlich weder nach Rundfunkteilnehmern und Nichtteilnehmern, noch nach solchen Rundfunkteilnehmern, die ihre Gebühren ordnungsgemäß entrichten oder solchen, die dies unterlassen, gegliedert. Ein gezieltes Zugreifen der GEZ auf Personen, die ihrer Gebührenpflicht nicht nachkommen, wird weder ermöglicht noch erkennbar gefördert. So könnte die GEZ beispielsweise nicht ohne weiteres an alle diejenigen herantreten, deren Daten ihr übermittelt wurden und für die ihr keine Gebührenmeldung vorliegt. Dem stehen nach meiner Kenntnis die entsprechenden Bestimmungen in den Rundfunkgebührenstaatsverträgen entgegen. Die Auskunftsberechtigung der GEZ setzt danach die begründete Vermutung des Schwarzempfangs voraus. Dafür liefert die regelmäßige Meldedatenübermittlung aber keine Anhaltspunkte.

Demgegenüber sehe ich in einer solchen Vorgehensweise eine deutliche Berührung des informationellen Selbstbestimmungsrechts der betroffenen Bürger. Aufgrund der Möglichkeiten der modernen Datenverarbeitung ist nicht auszuschließen, daß bei der GEZ ein - wenn auch verkürztes - Bundeseinwohnerregister entsteht, das Auswertungen des Bürgerverhaltens im Verhältnis zu Medien zuläßt, die mit dem eigentlichen Zweck der Übermittlung nichts gemein haben (z. B. Werbung und Marktforschung oder namentliche Feststellung von Personen, die bestimmte Medien nicht in Anspruch nehmen). Ich bezweifle, daß dem mit dem Versuch einer Begrenzung der Verwendung zu Zwecken der Ermittlung, wie ihn z. B. die nordrhein-westfälische

Verordnung vorsieht, wirksam begegnet werden kann. Gerade weil der undifferenzierte Charakter der Einwohnerdaten eine zielgerichtete Ermittlung nicht zuläßt, ist dieses Merkmal wenig geeignet, den Verwendungszweck hinreichend zu bestimmen.

Argumenten, die Übermittlung der Daten bereits gemeldeter Rundfunkteilnehmer könne diese nicht beeinträchtigen, da sie anzeigepflichtig seien, kann weder sachlich noch rechtlich gefolgt werden. Die Übermittlung von Daten ohne Kenntnis der Betroffenen greift grundsätzlich in deren informationelles Selbstbestimmungsrecht (vgl. Art. 33 SächsV, § 1 SächsDSG) ein.
Hinsichtlich der Rundfunkteilnehmer, die ihre Geräte bereits angemeldet haben bzw. die nicht gebührenpflichtig sind (z. B. volljährige Kinder ohne eigenes Einkommen, Schwerbehinderte und Sozialleistungsempfänger), ist die Übermittlung zum Zweck "Feststellung von Schwarzhörern und -sehern" nicht erforderlich. Dieser Teilnehmerkreis stellt jedoch weitaus die große Mehrzahl dar. Nutzeffekte, wie "laufende Aktualisierung des Adressenbestandes", "Tätigkeit des Außendienstes", "allgemeine Werbemaßnahmen" rechtfertigen den damit verbundenen Eingriff in das informationelle Selbstbestimmungsrecht nicht.

Nach alledem halte ich eine regelmäßige Meldedatenübermittlung an die GEZ für unverhältnismäßig und für mit Art. 33 SächsV, § 1 SächsDSG nicht vereinbar.

5.4 Personenstandsbücher und Ahnenforschung

Bei den Personenstandsbehörden mehren sich Anfragen genealogisch forschender Bürger. Ich habe den Petenten sowie dem für das Personenstandsrecht zuständigen Bundesministerium des Innern mitgeteilt, daß die entsprechenden Auskunftsersuchen, die ich im Hinblick auf das angestrebte Zusammenwachsen der beiden ehemals getrennten Teile Deutschlands oftmals für sinnvoll und notwendig halte, wegen der gegenwärtigen Rechtslage teilweise nur unbefriedigend oder abschlägig beantwortet werden können.

Im einzelnen gilt folgendes:
Nach § 61 Abs. 1 Personenstandsgesetz (PStG) darf Privatpersonen Einsicht in bzw. Durchsicht von Personenstandsbüchern (oder Auskunft daraus) nur gewährt werden, soweit sich der Eintrag auf den Ehegatten oder Vorfahren oder auf Abkömmlinge der *geraden Linie* bezieht. Vom Standesamt können daher z. B. Auskünfte über Eltern und Großeltern (gerade Linie), nicht aber über deren weitere Kinder und Kindeskinder (Seitenlinie) erteilt werden. Für Verwandte der Seitenlinie ist nach § 61 Abs. 1 Satz 3 PStG die Nutzung von Personenstandsbüchern nur dann zulässig, wenn der Auskunftssuchende ein *rechtliches* Interesse geltend machen kann. Die Einsichtnahme in die Personenstandsbücher ist deswegen nach der (merkwürdigerweise sehr restriktiven) Rechtsprechung nur erlaubt, wenn sie zur Verfolgung von Rechten oder zur Abwehr von Ansprüchen notwendig ist. Hierunter fällt die allgemeine Einsichtnahme in Personenstandsunterlagen im Rahmen der genealogischen Forschung *nicht.*

Insbesondere treten dann Probleme auf, wenn ein Verstorbener keine Abkömmlinge hat oder Abkömmlinge bereits verstorben sind. Denn in diesem Fall sind keine berechtigten Personen vorhanden, die Vollmachten zur Einsicht in die Personenstandsbücher erteilen könnten.

Ich habe daher gegenüber dem Bundesministerium des Innern eine nach meinem Kenntnisstand diskutierte Neufassung des § 61 Abs. 1 PStG begrüßt, wonach zur Einsichtnahme ein *berechtigtes* Interesse (das ist jedes von der Rechtsordnung erlaubte Interesse, also auch genealogische Forschung) genügt, wenn seit dem Tod des Betroffenen mindestens 30 Jahre oder seit seiner Geburt mindestens 120 Jahre vergangen sind.

5.5 Kommunale Selbstverwaltung

5.5.1 Rechtliche Entwicklung

Die bislang noch in Sachsen gültige Kommunalverfassung von 1990 ist durch die jetzt verabschiedete Sächsischen Gemeindeordnung abgelöst worden. Aus datenschutzrechtlicher Sicht ist zu begrüßen, daß die Gemeindeordnung Verschwiegenheitspflichten ehrenamtlich tätiger Bürger, insbesondere aber auch der Gemeinderäte und der Bürgermeister, vorsieht. Auch die Behandlung von Beratungsgegenständen, die geeignet sind, schutzwürdige Interessen Einzelner zu beeinträchtigen, in *nichtöffentlicher* Sitzung, sowie die Behandlung von Niederschriften aus nichtöffentlichen Sitzungen, sollen datenschutzgerecht geregelt werden.

5.5.2 Nichtöffentliche Gemeinderatssitzungen

Wiederholt wurde gefragt, welche Beratungsgegenstände in *nichtöffentlicher* Gemeinde-ratssitzung zu behandeln sind. Hierzu habe ich mitgeteilt, daß die Gemeindeordnungen der anderen Bundesländer sowie die sächsischen Entwürfe der jetzigen Gemeindeordnung fast wortgleich vorsehen, daß Gemeinderatssitzungen *grundsätzlich öffentlich* - also für jedermann zugänglich - abzuhalten sind. Dieser Grundsatz soll das kommunale Handeln für die Bürger transparent machen.

Der Öffentlichkeitsgrundsatz ist jedoch einzuschränken, und auch hier befindet sich die Sächsische Gemeindeordnung mit den Gemeindeordnungen der alten Bundesländer im Einklang, sofern das öffentliche Wohl oder berechtigte Interessen Einzelner eine nichtöffentliche Behandlung erfordern. Soweit demnach Beratungsgegenstände das Recht auf informationelle Selbstbestimmung und damit die schutzwürdigen Belange eines Betroffenen beeinträchtigen können, ist die Öffentlichkeit auszuschließen (z. B. bei Personalentscheidungen, Grundstücksangelegenheiten, Steuerangelegenheiten, Erörterung persönlicher oder wirtschaftlicher Verhältnisse, Zuschußgewährung an einzelne Personen, Rechtsstreitigkeiten zwischen Gemeinde und Bürger). Zusammenfassend: Die Ergebnisse *öffentlicher* Sitzungen (in denen regelmäßig auch Pressevertreter zu finden sind) dürfen veröffentlicht werden. Demzufolge ist die

Veröffentlichung der Beratungsergebnisse aus *nichtöffentlichen* Sitzungen unbeschadet sonstiger Geheimhaltungsgründe *unzulässig*, solange das Recht auf informationelle Selbstbestimmung einzelner beeinträchtigt werden kann. Bei zu vermutender Verletzung des informationellen Selbstbestimmungsrechts scheidet die Bekanntgabe dieser Ergebnisse auf Dauer aus.

5.5.3 Presseerklärungen der Verwaltung über Stasi-Belastete

In jüngster Zeit häufen sich Anfragen Betroffener und von Behörden, ob und ggf. unter welchen Voraussetzungen die Presse (und damit die Öffentlichkeit) über "Stasi"-belastete Gemeinderatsmitglieder bzw. Gemeindebedienstete durch die Verwaltung informiert werden darf.

Hierzu vertrete ich die Auffassung, daß das allgemeine Persönlichkeitsrecht z. B. durch das Grundrecht auf Meinungs- und Pressefreiheit (Art. 5 Abs. 1 GG) Einschränkungen erfährt. Der verfassungsrechtliche Persönlichkeitsschutz wirkt nämlich nicht absolut, soweit es nicht um den Kernbereich *privater* Lebensgestaltung geht (BGH NJW 1988, 1016 f.). Wenn es zur Meinungsbildung in einer die Öffentlichkeit interessierenden Frage beiträgt, können die schutzwürdigen Belange der persönlichen Eigensphäre zurückgedrängt werden. Unter diesem Gesichtspunkt ergibt sich insbesondere für Persönlichkeiten des öffentlichen Lebens als Personen der Zeitgeschichte eine Einschränkung des Schutzes der Privatsphäre sowie des in Art. 33 Sächsische Verfassung und § 1 Sächsisches Datenschutzgesetz statuierten Rechts auf informationelle Selbstbestimmung.

Stadtverordnete, Gemeinderäte, Beigeordnete, Dezernenten und Amtsleiter in herausgehobener Position (nicht aber nachgeordnete Bedienstete) sind solche Persönlichkeiten des öffentlichen Lebens mit "verkürztem" Persönlichkeitsschutz. Dieser Personenkreis muß damit rechnen, daß sich das Informationsinteresse der Bürger nicht nur auf günstig zu bewertende Handlungen oder Ereignisse erstreckt. Die Unterrichtung der Presse über die "Stasi"-Vergangenheit, die Abwahl und die Entlassung der Betroffenen, kann - soweit sie nicht sachlich falsch oder hämisch ist - nicht beanstandet werden.

5.5.4 Unterrichtung der Presse über Ordnungswidrigkeiten von Mandatsträgern

Eine Eingabe veranlaßte mich zu prüfen, unter welchen Voraussetzungen die Verwaltung die Presse über angeblich begangene Ordnungswidrigkeiten von Abgeordneten unterrichten darf.

Hierzu vertrete ich folgende Auffassung:

Nach § 4 Abs. 1 Sächsisches Gesetz über die Presse (Pressegesetz) sind Behörden verpflichtet, den Vertretern der Presse zur Erfüllung von deren öffentlicher Aufgabe Auskünfte zu erteilen. Zu diesem Aufgabenbereich gehört gemäß § 3 Abs. 2 Pressegesetz die Beschaffung und Verbreitung von Nachrichten in Angelegenheiten von öffentlichem Interesse. Steht ein Abgeordneter im Verdacht, eine nicht völlig bedeutungslose Ordnungswidrigkeit begangen zu haben, handelt es sich stets um eine Angelegenheit von öffentlichem Interesse, da die Bevölkerung das Recht hat, über das Verhalten ihrer politischen Vertreter, auch über deren Wirkungsbereich als Mandatsträger hinaus, informiert zu werden. Allerdings ist im Pressegesetz nicht geregelt, unter welchen Voraussetzungen eine Behörde der Presse *von sich aus* Mitteilungen machen darf.

Die Zulässigkeit der Datenübermittlung richtet sich bei dieser Sachlage nach dem Grundgedanken des § 15 Abs. 1 Nr. 2 Sächsisches Datenschutzgesetz (Datenübermittlung an nicht-öffentliche Stellen), wonach das schutzwürdige Interesse des Betroffenen am Unterbleiben der Übermittlung gegen das Interesse des Empfängers (Presse) an der Kenntnis der Daten abgewogen werden muß. Dabei ist zu berücksichtigen, daß sowohl die Pressefreiheit als auch das Recht auf informationelle Selbstbestimmung verfassungsmäßig garantiert sind. Daher muß für die Bestimmung der Schranken der Pressefreiheit das Recht auf informationelle Selbstbestimmung beachtet werden; auf der anderen Seite sind die Schranken des Rechts auf informationelle Selbstbestimmung im Lichte der besonderen Bedeutung der Pressefreiheit zu bestimmen.

Hieraus ergibt sich, daß das Persönlichkeitsrecht des einzelnen zurückgedrängt werden kann, soweit eine Presseveröffentlichung zur Meinungsbildung in einer die Öffentlichkeit wesentlich interessierenden Frage beiträgt. Unter diesem Gesichtspunkt erfährt insbesondere das Recht auf informationelle Selbstbestimmung von Personen des öffentlichen Lebens (Abgeordnete) eine Einschränkung. Letztendlich muß im Einzelfall entschieden werden, wann eine Weitergabe von Informationen seitens der Behörde an die Presse gerechtfertigt ist. Hierbei spielt die Schwere der vorgeworfenen Ordnungswidrigkeit die entscheidende Rolle.

5.5.5 Personenbezogene Daten in kommunalen Mitteilungsblättern

Bei einer Bürgermeisterversammlung wurde ich mit der offensichtlich gängigen Praxis konfrontiert, in kommunalen Mitteilungsblättern personenbezogene Daten über

- Zu- und Wegzüge
- Geburten
- Eheschließungen
- Sterbefälle
- Gewerbean- und abmeldungen

zu veröffentlichen. Aus datenschutzrechtlicher, melderechtlicher, personenstandsrechtlicher und gewerberechtlicher Sicht sind solche Veröffentlichungen *ohne (vorherige) schriftliche Einwilligung* der Betroffenen *unzulässig*.

5.5.6 Verwendung von Postkarten im Schriftverkehr mit Bürgern

Eine Meldebehörde hat einen Bürger mittels Postkarte aufgefordert, sich anzumelden (Nichtanmeldung stellt eine Ordnungswidrigkeit dar). Ich habe die Behörde aufgefordert, Schreiben mit personenbezogenen Daten künftig in verschlossenen Umschlägen zu versenden. Nach § 9 Abs. 2 Nr. 2 SächsDSG haben öffentliche Stellen zu gewährleisten, daß Datenträger mit personenbezogenen Angaben nicht von Unbefugten gelesen werden können. Postkarten erfüllen dieses Erfordernis nicht. Auch wenn die Bundespost den Transport nach den Bestimmungen der Postordnung und entsprechend dem Postgeheimnis durchführt, schließt dies nicht aus, daß Personen unbefugt Kenntnis von einem Verwaltungsvorgang nehmen können, wenn Briefkästen gemeinsam von Familienmitgliedern oder Hausbewohnern benutzt werden oder bei längerer Abwesenheit Nachbarn mit der Leerung des Briefkastens beauftragt werden.

5.6 Baurecht

5.6.1 Veröffentlichung von Bauherrendaten

Ich hatte mich mit der Frage zu befassen, unter welchen Voraussetzungen Bauherrendaten von der Baugenehmigungsbehörde an Baustelleninformationsdienste oder zum Zwecke der Veröffentlichung im Amtsblatt übermittelt werden dürfen.

Grundsätzlich ist eine Datenübermittlung nach § 4 Abs. 1 Nr. 1 SächsDSG nur zulässig, wenn sie das Sächsische Datenschutzgesetz selbst oder eine andere Rechtsnorm erlaubt. Da durch eine Weitergabe der Bauherrendaten an Private bzw. durch die Veröffentlichung sehr wohl schutzwürdige Belange der Betroffenen beeinträchtigt werden können (z. B. unerbetene massive Werbung für Bauprodukte, Gartenartikel und Einrichtungsgegenstände, unerwünschte Vertreterbesuche u. ä.), kommt eine Datenübermittlung nach § 15 Abs. 1 Nr. 2 SächsDSG nicht in Betracht. Nach dieser Bestimmung ist die Datenübermittlung an nicht-öffentliche Stellen zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse am Unterbleiben der Übermittlung hat. Auch die Sächsische Bauordnung sieht keine entsprechende bereichsspezifische Rechtsnorm für eine Bekanntgabe von Bauherrendaten vor. Deshalb ist eine Datenübermittlung nur unter den Voraussetzungen des § 4 Abs. 1 Nr. 2 und Abs. 2, 3 SächsDSG, also nur mit (vorheriger) schriftlicher Einwilligung des Betroffenen zulässig.

Die mir vorliegenden Bauantragsformulare sehen zwar eine Einwilligungsformel vor, die jedoch unterschiedlich interpretiert wird.
Der Betroffene hat die Möglichkeit, zur Frage der Datenübermittlung auf den Formularen entweder ein "Ja"- oder ein "Nein"-Kästchen anzukreuzen. Problematisch ist hierbei der Fall, wenn der Bauherr bzw. der Entwurfsverfasser das Antragsformular zu diesem Punkt nicht ausfüllt. Das Staatsministerium des Innern hat hierzu den Standpunkt vertreten, daß eine Weitergabe der Daten auch in diesem Fall zulässig sei, da der Betroffene einer Veröffentlichung ausdrücklich widersprechen müßte. Diese Auffassung ist nicht mit dem Sächsischen Datenschutzgesetz vereinbar. Es handelt sich nämlich bei der datenschutzrechtlichen Einwilligung gemäß § 4 SächsDSG um eine empfangsbedürftige Willenserklärung. Kreuzt der Betroffene weder "Ja" noch "Nein" an, äußert er überhaupt keinen Willen, so daß ein wesentliches Begriffsmerkmal für das Vorliegen einer Willenserklärung fehlt. Ich habe dem Staatsministerium des Innern deshalb mitgeteilt, daß die Übermittlung der Bauherrendaten unzulässig ist, wenn der Betroffene weder das Ja-Kästchen noch das Nein-Kästchen angekreuzt und damit seine Einwilligung nicht erteilt hat.
Damit künftig Fehlinterpretationen ausgeschlossen sind, werde ich mich für eine datenschutzgerechte Vordruckgestaltung einsetzen.

5.6.2 Stadtsanierung

Für Maßnahmen der Stadtsanierung haben mehrere Gemeinden Verträge mit einer Sanierungsgesellschaft geschlossen. Die Verträge verpflichten die Gesellschaft u. a., nach §§ 138 ff. Baugesetzbuch (BauGB) treuhänderisch für die Gemeinden tätig zu werden - also die vorbereitenden Untersuchungen durchzuführen und die Sanierungsmaßnahmen zu betreuen. Damit führt die Sanierungsgesellschaft eine Datenverarbeitung im Auftrag nach § 7 SächsDSG durch.
Ich war gebeten worden, die verwendeten Fragebogen datenschutzrechtlich zu beurteilen.
Im einzelnen habe ich folgendes festgestellt:
Nach § 11 Abs. 2 SächsDSG ist bei der Erhebung von Daten die Rechtsvorschrift anzugeben, die den Betroffenen zur Auskunft verpflichtet. Obwohl § 138 BauGB eine solche Auskunftspflicht im Zusammenhang mit vorbereitenden Sanierungsmaßnahmen vorsieht, fehlte in allen verwendeten Fragebogen ein Hinweis auf diese die Auskunftspflicht begründende Rechtsvorschrift und die Folgen bei der Verweigerung von Angaben.
Die Fragen im *Gebäude- und Grundstücksbogen* habe ich in ihrer Gesamtheit für erforderlich gehalten, um die Sanierungsbedürftigkeit eines Gebietes beurteilen zu können.
Die Frage im *Haushaltsbogen* nach der Nationalität des Betroffenen habe ich als unzulässig angesehen, da sie kein geeignetes Merkmal darstellt, um auf die Sanierungsbedürftigkeit eines Stadtteils schließen zu können. Eine solche Frage könnte den Eindruck erwecken, daß aufgrund von Vorurteilen ein hoher Sanierungsbedarf unterstellt wird, wenn der Stadtteil vorwiegend von Ausländern bestimmter Nationalitäten bewohnt wird.

In den Verträgen zwischen den Gemeinden und der Sanierungsgesellschaft war nicht vorgesehen, Daten über soziale Verhältnisse zu erheben. Obwohl § 138 Abs. 1 BauGB durchaus eine ausreichende Rechtsgrundlage dafür bilden würde, habe ich sämtliche Fragen dieser Art für unzulässig gehalten, da sie über den Auftrag im Treuhandvertrag hinausgingen. Außerdem sollten die Daten über soziale Verhältnisse von Haushaltsmitgliedern beim Haushaltsvorstand erhoben werden. Ich habe darin eine gesetzwidrige Form der Datenerhebung bei Dritten gesehen, da § 11 Abs. 2 SächsDSG die Erhebung personenbezogener Daten beim Betroffenen mit seiner Kenntnis vorschreibt.
Für die in den Abschnitten "Mitwirkungsbereitschaft an der Sanierung" und "nur für Mieter" gestellten Fragen nach persönlichen Einschätzungen und Ansichten habe ich einen Hinweis auf die Freiwilligkeit dieser Angaben für erforderlich gehalten.
Auch die im *Betriebsbogen* an den Betriebsinhaber gerichteten Fragen nach Einschätzungen zu der künftigen Betriebsentwicklung habe ich weder durch § 138 BauGB gedeckt gesehen noch durch den Auftrag im Treuhändervertrag.
Die Sanierungsgesellschaft teilt meine datenschutzrechtliche Beurteilung nicht. Sie ist der Auffassung, die Durchführung der vorbereitenden Untersuchungen werde durch die datenschutzrechtlichen Anforderungen unmöglich gemacht. Denn nunmehr könnten nur noch Untersuchungsergebnisse erzielt werden, die ohne Aussagekraft und deshalb wertlos seien. Ich teile diese Bewertung nicht.
Zwischenzeitlich hat die Sanierungsgesellschaft das Sächsische Staatsministerium des Innern eingeschaltet, um über diese Stelle eine Lösung der Probleme zu erreichen, die durch eine von "Informationsdefiziten ausgelöste ungerechtfertigte Betrachtungsweise" des Datenschutzbeauftragten entstanden seien. Von dort habe ich leider keine Stellungnahme erhalten.
Ich verfolge die Angelegenheit weiter.

5.6.3 Informationelles Selbstbestimmungrecht bei der Wohnungsbauförderung

Im Verfahren zur Förderung des Wohnungsbaus gewährt der Freistaat Sachsen Bauherren unter bestimmten Voraussetzungen Zuwendungen für den Bau von Mietwohnungen oder für andere Baumaßnahmen, "um eine bedarfsgerechte Wohnraumversorgung der Bevölkerung langfristig sicherzustellen". Zur Prüfung der Förderungsfähigkeit der einzelnen Vorhaben müssen die Antragsteller auf Antragsformularen u. a. Angaben zu ihren Einkommensverhältnisses machen. Nach einer Verwaltungsvorschrift des Sächsischen Staatsministeriums des Innern (SMI) hat die Gemeindeverwaltung die Anträge entgegenzunehmen und sie an die zuständigen Wohnungsbauförderungsstellen weiterzuleiten. Das Bürgermeisteramt prüft in dem Verfahren die Anträge auf Vollständigkeit von Unterlagen und Angaben.

In einer Eingabe beschwert sich ein Betroffener darüber, daß seine Einkommensverhältnisse bei Vorlage des Antrags zur Wohnungsbauförderung auch dem Bürgermeister bekannt würden. Er befürchtet, daß hierdurch, insbesondere bei kleineren Gemeinden, schutzwürdige Interessen beeinträchtigt werden könnten.

Ich habe dem Petenten und dem Sächsischen Staatsministerium des Innern mitgeteilt, daß es sich bei Eigentums- und Finanzverhältnissen um geschützte persönliche Daten handelt, deren Kenntnisnahme durch die Bediensteten der Gemeinden das informationelle Selbstbestimmungsrecht der Betroffenen beeinträchtigen können. Nach Art. 33 Sächsische Verfassung i. V. m. den Grundsätzen des "Volkszählungsurteils" ist ein Eingriff in das informationelle Selbstbestimmungsrecht des Einzelnen nur auf Grund von Rechtsnormen als Ergebnis einer parlamentarischen Mehrheit zulässig. Der Erlaß einer Verwaltungsvorschrift genügt diesen Anforderungen nicht, da es sich hierbei - im Gegensatz zu Gesetzen - nur um verwaltungsinterne Regelungen ohne Außenwirkung handelt.

Außerdem habe ich darauf hingewiesen, daß nicht alle Angaben auf dem verwendeten Antragsformular zur Aufgabenerfüllung der Gemeinde erforderlich sind. Das Bürgermeisteramt hat in dem Verfahren nicht die Befugnis, die angegebenen Daten im Hinblick auf die Förderungsfähigkeit von Vorhaben inhaltlich auszuwerten, sondern prüft lediglich die Vollständigkeit der Unterlagen und Angaben. Hierzu wäre es ausreichend, der Gemeinde lediglich Kenntnis von persönlichen Daten (Anschrift des Bauherren, Lage des Grundstücks etc.), jedoch nicht von sensiblen sachlichen Daten (z. B. Einkommensverhältnisse) zu geben; insoweit fehlt der Gemeinde das Fachwissen, um die Daten auf Vollständigkeit zu prüfen.

Weiterhin entspricht das in dem Verfahren verwendete Antragsformular nicht den Anforderungen des § 11 Abs. 2 Sächsisches Datenschutzgesetz, wonach den Betroffenen der Erhebungszweck und die Rechtsvorschrift, die zur Auskunft verpflichtet, mitzuteilen ist. Des weiteren ist der Betroffene über die Folgen der Verweigerung der Angaben aufzuklären. Ein diesbezüglicher Hinweis fehlt auf dem Formular.

Ich habe das Sächsische Staatsministerium des Innern gebeten, unter Beachtung der von mir geäußerten Bedenken einen Weg aufzuzeigen, wie das Verfahren datenschutzgerecht ausgestaltet werden könnte. Ich erwarte, daß das SMI hier alsbald reagiert.

5.6.4 Datensammlung "Wohnungspolitik"

Die ehemaligen Datenverarbeitungszentralen (DVZ) in Sachsen haben neben einer Reihe von Dateien auch einen Datenspeicher "Wohnungspolitik" (WOPOL) geführt, der bis zum Ende des Jahres 1990 ständig aktualisiert wurde.

Kernstück des Datenspeichers WOPOL bildeten die folgenden Dateien:

- *Wohnungsdatei* mit Informationen zur Lage, Größe, Ausstattung und zum Mietpreis einer Wohnung,

- *Gebäudedatei* mit Angaben zum Eigentümer oder Verwalter, zum Baujahr und Bauzustand einschließlich Bauausführung, zur Grundstücksgröße mit den Gebäudemaßen, zur Wasser- und Abwasserversorgung, Art der Energieversorgung, zu Telefonanschlüssen usw.

Diese beiden Stammdateien wurden je nach Anforderung für die unterschiedlichsten Aufgaben genutzt. Regelmäßig wurde jedoch unter Einbeziehung der *Bewohnerdatei*, die einen aktuellen Auszug aus der Einwohnermeldedatei darstellte, eine *Wohnungsbelegungsdatei* erstellt. Diese enthielt als Ergebnis aus der Verknüpfung neben ausgewählten Gebäudedaten folgende statistische Angaben für jede Wohnung: Anzahl der Personen, Anzahl der Kinder unter 17 Jahren, Anzahl der Altersrentner und der Personen über 70 Jahren, Anzahl der Haushalte mit Anzahl der Personen und Kinder pro Haushalt.

Die genannten Dateien sind Altdatenbestände im Sinne des § 35 SächsDSG. Sie wurden entsprechend meiner Bekanntmachung vom 20. Februar 1992 (vgl. Nr. 16.1.1) von den Datenverarbeitungszentralen vorläufig unter Verschluß genommen.

Nach der Privatisierung des ehemaligen DVZ Sachsen in Dresden bat die Stadt Dresden um Freigabe der Wohnungsbelegungsdatei, um ein Rahmenkonzept für die Stadtentwicklung erstellen zu können (Ermittlung des gesamtstädtischen Wohnungsbedarfs, Planung der sozialen Infrastruktur, Feststellung der Ver- und Entsorgungssituation, Bevölkerungsprognose). Ich habe die Freigabe an die Bedingung geknüpft, daß die Datei vorab so aufbereitet wird, daß die kleinste statistische Einheit nicht die Wohnung, sondern die Blockseite darstellt. (Eine Blockseite ist ein Straßenteil mit gleichem Straßennamen, der durch zwei Einmündungen begrenzt ist.) Nur durch diese Auflage habe ich einen ausreichenden Schutz vor der Reanonymisierung der Daten gesehen, die durch Verknüpfung mit der aktuellen Einwohnermeldedatei problemlos möglich wäre.

5.7 Statistikgesetz

Die Staatsregierung hat im Juni 1992 den Entwurf eines Sächsischen Statistikgesetzes in den Landtag eingebracht (Drucks. 1/2063), der im Juli 1992 an den Innenausschuß überwiesen worden ist. Über den Gesetzentwurf wurde noch nicht abschließend beraten.

Das Staatsministerium des Innern berücksichtigte im Entwurf im wesentlichen meine Forderungen. Über sie war im April 1992 in einem eingehenden Sachgespräch verhandelt worden. Folgende wesentlichen Änderungen wurden gegenüber dem Entwurf vom März 1992 vorgenommen:

- Bei § 1, der die Grundsätze der amtlichen Statistik festlegt, wurde eingefügt, daß die amtliche Statistik unter Beachtung des Grundrechts auf informationelle Selbstbestimmung zu führen ist. Ferner wird die Privatsphäre grundsätzlich geschützt und der Grundsatz einer frühestmöglichen Anonymisierung aller personenbezogenen Informationen betont.

- Der Entwurf geht auf Grund meiner Forderung erfreulicherweise davon aus, daß die für die amtliche Statistik erhobenen Einzelangaben ausschließlich Zwecken dienen, die eine Rechtsvorschrift, also ein Gesetz, eine Verordnung oder eine Satzung vorsehen. Ursprünglich war die Bestimmung vorgesehen, daß Landesstatistiken ohne Auskunftspflicht durch bloße Verwaltungsvorschrift bzw. auf Beschluß der Gemeindevertretung angeordnet werden können. Diese großzügigen Ausnahmen wären jedoch der Bedeutung statistischer Erhebungen und ihrer Auswirkungen auf die Bürger nicht gerecht geworden. Ganz besonders die neuen Bundesländer müssen darauf achten, daß die Bürger nicht von einer Flut statistischer Erhebungen überschwemmt werden. Die Statistik erfüllt im Rechtsstaat und in der sozialen Marktwirtschaft, anders als in der DDR, eine wesentlich zurückhaltendere Rolle. Auch ohne Auskunftspflicht fühlt sich der Bürger vielfach als Objekt von Befragungsaktionen bedrängt. Ist eine Erhebung tatsächlich notwendig, so kann sie jederzeit durch Rechtsvorschrift angeordnet werden, an die allerdings höhere Anforderungen als an eine bloße Verwaltungsentscheidung zu stellen sind. Der Praxis wird im übrigen dadurch Genüge geleistet, als Landesstatistiken mit Angaben aus allgemein zugänglichen Quellen, aus öffentlichen Registern (mit Zugangsrecht des Statistischen Landesamtes) und Statistiken im (und für den) Verwaltungsvollzug keiner Rechtsvorschrift bedürfen.

Bei der weiteren Erörterung des Gesetzentwurfs im Innenausschuß des Landtags werde ich u. a. darauf hinwirken, daß die Bestimmung des § 8 Abs. 2 geändert wird. Danach sind Kommunalstatistiken mit Auskunftspflicht nur zulässig, wenn das statistische Material vom Statistischen Landesamt nicht zur Verfügung gestellt werden kann. Nicht einzusehen ist, weshalb bei den Kommunen statistische Erhebungen ohne Auskunftspflicht selbst dann zulässig sein sollen, wenn sie die benötigten Daten vom Statistischen Landesamt zur Verfügung gestellt bekommen können.

5.8 Archivwesen

Die Staatsregierung hat dem Landtag im Dezember 1992 den Entwurf eines Archivgesetzes für den Freistaat Sachsen (Landtagsdrucksache 1/2476) vorgelegt. Der vom federführenden Staatsministerium des Innern erarbeitete Entwurf war mit mir in den Grundzügen abgestimmt worden. Berücksichtigt wurden erfreulicherweise u. a. meine nachfolgenden Forderungen:

- Es wurde eine unmittelbare gesetzliche Verpflichtung festgelegt, wonach die staatlichen Archive nach der Übernahme des Archivgutes die schutzwürdigen Belange Betroffener, insbesondere hinsichtlich der personenbezogenen Unterlagen, zu beachten haben.

- Für die einzuhaltenden Fristen (im Regelfall Nutzungsfreigabe 30 Jahre nach Entstehung der Unterlagen, bei personenbezogenem Archivgut 10 Jahre nach dem Tod der betroffenen Person) ist das Wort "Schutzfrist" anstelle des Wortes "Sperrfrist" verwendet worden, da dies den Zweck der Frist besser zum Ausdruck bringt.
- Da für das vom Bund übernommene Archivgut Bundesrecht anzuwenden ist, wurde hierfür eine spezielle Vorschrift festgelegt, die allerdings noch der Konkretisierung bedarf.
- Die Schutzfristen für personenbezogenes Archivgut gelten nicht für Archivalien, die sich auf die Tätigkeiten von Personen in Ausübung ihrer öffentlichen Ämter bzw. in SED-beeinflußten Funktionen beziehen. Auf diese Bestimmung lege ich ganz besonderen Wert, da der Erforschung der nationalsozialistischen und der kommunistischen Gewaltherrschaft keine datenschutzrechtlichen Hindernisse in den Weg gestellt werden dürfen. Die Person des Amtsträgers tritt hinter der amtlichen Tätigkeit zurück; sie ist deshalb datenschutzrechtlich nicht schutzwürdig. Datenschutz darf nicht dazu dienen, staatliches Unrecht zu verschleiern.
- Den kommunalen Archiven und den sonstigen öffentlichen Archiven wird vorgeschrieben, daß sie die wesentlichen Vorschriften, wie sie von den staatlichen Archiven einzuhalten sind, zu beachten haben.

Im Zusammenhang mit der Altdatenbearbeitung stellte sich die Frage des Einsichtsrechts Betroffener. Die Staatsregierung hatte auf meine Anregung hin schon in ihrer Antwort auf die Große Anfrage der CDU-Fraktion "Sicherung von Akten über Korruption und Amtsmißbrauch" (Landtagsdrucksache 1/2360; vgl. oben 1.3.3) festgestellt, daß es einer gesonderten gesetzlichen Regelung für die Fälle bedürfe, in denen der Betroffene bei Einsichtnahme, z.B. in seine Ausreiseakte, auf Namen von Personen stoßen würde, die zu seinem Nachteil Informationen an Funktionsträger geliefert haben. Darüber, daß Funktionsträger in dieser Eigenschaft nicht geschützt werden sollen, bestand ohnehin Einigkeit. Letzter Stand der Verhandlungen ist, daß ein von mir angeregter Entwurf einer Änderung des § 6 (Rechtsansprüche Betroffener) dem Innenausschuß des Landtages zur Annahme empfohlen werden soll. Danach hat jedermann des Recht, vom zuständigen staatlichen Archiv Auskunft darüber zu verlangen, ob in dem staatlichen Archivgut, das auch Archivgut der Parteien und Organisationen aus der Zeit nach dem 2. Weltkrieg enthält, Daten zu seiner Person enthalten sind, soweit das Archivgut durch Namen erschlossen ist oder sonst mit vertretbarem Aufwand ermittelt werden kann. Ist das der Fall, hat er das Recht auf Einsicht und Herausgabe von Kopien der Unterlagen. Fazit dieser vorgeschlagenen Bestimmung: Jedermann hat in ähnlicher Weise wie nach dem Stasiunterlagengesetz ein volles Einsichtsrecht in die ihn betreffenden Vorgänge aus der Zeit der SED-Diktatur.

5.9 Landessystemkonzept

Das Staatsministerium des Innern bemüht sich um ein Konzept zur Verbesserung der Verwaltungstätigkeit im Freistaat Sachsen durch effektiven Informationsaustausch. Zu diesem Zweck hat es die Gesellschaft für Mathematik und Datenverarbeitung beauftragt, eine Studie anzufertigen, die zunächst die Ausgangssituation und die Kommunikationsbeziehungen zwischen den jeweiligen Ressorts analysieren soll. Dazu müssen die Fachressorts den aktuellen und den zu erwartenden Informations- und Kommunikationsbedarf im eigenen Haus und in den nachgeordneten Dienststellen angeben. Anhand des dabei ermittelten Bedarfs und aufgrund einer fachkundigen Kosten-Nutzen-Analyse soll entschieden werden, ob ein ressortübergreifendes landesweites Datennetz installiert werden soll.

Sollte die Entscheidung zugunsten des landesweiten Netzes fallen, ist bei seinem Aufbau der Informationssicherheit besondere Beachtung zu schenken. Das betrifft in erster Linie die:

- *Vertraulichkeit, Abhörsicherheit und Anonymität* (Schutz personenbezogener Daten, Anonymität der Nutz- und Vermittlungsdaten zum Schutz von Verkehrsflußanalysen)
- *Kommunikationsintegrität* (Authentifizierung, Partnergewißheit, Zugangs- und Zugriffskontrolle, Integrität der gesendeten Daten, Sende- und Empfangsnachweis)
- *Verbindlichkeit* (Nachweisbarkeit von Kommunikationsvorgängen zur Beweissicherheit und Protokollierung)
- *Verfügbarkeit* (Funktionalität, Betriebskontinuität).

Diese Forderungen gründen sich auf die Tatsache, daß bei einem landesweiten Netz wesentlich vielfältigere Zugriffsmöglichkeiten von Befugten und Unbefugten auf personenbezogene Daten auftreten können und damit die Mißbrauchsmöglichkeit erhöht wird. Bedeutende Gefährdungen gehen auch von einem Verlust der Integrität (Verarbeitung der Daten in vorgesehener Weise) sowie von unerlaubten Wechselbeziehungen zwischen solchen Sachgebieten, die voneinander abzuschotten sind, aus.
Um diese Risiken einzuschränken, müssen die gesetzlichen Bestimmungen strikt eingehalten werden, d.h. personenbezogene Daten dürfen nur verarbeitet (Erheben, Speichern, Verändern, Übermitteln, Nutzen, Sperren und Löschen) werden, wenn dies durch Rechtsvorschrift zugelassen ist.

Neben der Forderung nach erhöhter Effizienz der Verwaltung und Beschleunigung der Verwaltungsabläufe sind die Belange des Datenschutzes von Anbeginn, also bereits in der Projektierungsphase, voll zu berücksichtigen.

Bestrebungen in dem von den obersten Landesbehörden gebildeten Arbeitskreis Informationstechnik, nur einseitig, auf technische Vorteile bedacht, ein landesumfassendes Informations- und Kommunikationssystem zu installieren, werde ich entgegentreten. Dabei werde ich - wie bisher - nachdrücklich auf die Gefahren für das informationelle Selbstbestimmungsrecht eines jeden Bürgers aufmerksam machen.

5.10. Polizei

5.10.1 Polizeigesetz

Das Sächsische Polizeigesetz vom 30. Juli 1991 (SächsGVBl. S.291) enthält keine bereichsspezifischen, hinreichend bestimmten Rechtsgrundlagen für die polizeiliche Datenverarbeitung: Es verweist auf noch geltende Datenerhebungsvorschriften des in seinen übrigen Teilen aufgehobenen DDR-Gesetzes über die Aufgaben und Befugnisse der Polizei vom 13. September 1990 (GBl. S. 1489), das den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Anforderungen nicht genügt.

Das Grundrecht auf informationelle Selbstbestimmung, also die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, gilt selbstverständlich gerade auch gegenüber der Polizei. Auch polizeiliche Datenverarbeitung darf nur innerhalb der zulässigen Einschränkungen des Rechts auf informationelle Selbstbestimmung erfolgen. Diese Einschränkungen müssen normenklar sein, d. h., als Eingriffsnormen sind sie so präzise und verständlich wie möglich zu fassen, damit der Bürger wissen kann, wer was wann über ihn weiß. Nur wenn der Gesetzgeber dies beachtet, bleibt gewährleistet, daß sich der Einzelne nicht in seiner sozialen Handlungsfähigkeit einschränkt, weil er - so das Bundesverfassungsgericht - unsicher ist, welche seiner Verhaltensweisen jederzeit notiert, gespeichert, verwendet oder weitergegeben werden.
Hat ein die Eingriffsbefugnis der Polizei regelndes Polizeigesetz dieses verfassungsrechtliche Gebot zu beachten, so muß es zudem sämtlichen auf unterschiedlichen Rechtsgrundlagen beruhenden Sparten polizeilicher Aufgabenerfüllung Rechnung tragen: der Strafverfolgung, der vorbeugenden Bekämpfung von Straftaten und der Gefahrenabwehr.
Angesichts dieses gesetzlichen Änderungsbedarfs begrüße ich es, daß das Sächsische Staatsministerium des Innern sich jetzt mit einer Novellierung des Sächsischen Polizeigesetzes beschäftigt, wobei umfangreiche datenschutzrechtliche Regelungen vorgesehen sind. Ich wurde frühzeitig über diese Entwurfsarbeiten unterrichtet und habe dem Staatsministerium anhand konkreter Textvorschläge detailliert dargelegt, welche notwendigen datenschutzrechtlichen Vorkehrungen das Gesetz enthalten sollte.
Folgende Punkte sind hierbei hervorzuheben:

- Das Sächsische Polizeigesetz darf nicht den irrigen Eindruck entstehen lassen, mittels Datenverarbeitung könne *sämtlichen künftigen Straftaten* vorgebeugt werden. Die in diesem Bereich erforderliche Prognoseentscheidung der Polizei ist mit zahlreichen Unsicherheitsfaktoren verbunden. Die Gefahr, daß falsche Daten erhoben und gespeichert werden, besteht hier in besonderem Maße: Im Gegensatz zur Datenverarbeitung im Bereich der *Strafverfolgung,* bei der die Annahme eines Tatverdachtes der ständigen Überprüfung durch die Ermittlungen selbst unterzogen ist, fehlen Verifizierungs- und Falsifizierungsmaßnahmen bei der Datenverarbeitung zur vorbeugenden Straftatenbekämpfung in der Regel. Aus diesem Grunde sollten nur solchen Sachverhalte erfaßt werden dürfen, bei denen tatsächliche Anhaltspunkte für die Begehung von Straftaten eines gewissen Gewichts vorliegen. Denn unter dem Gesichtspunkt der Verhältnismäßigkeit muß geprüft werden, ob die Erhebung von Daten über potentielle Straftäter und sonstige Personen auch dann erforderlich ist, wenn es sich um Bagatellkriminalität handelt, z. B. Schwarzfahrten, kleine Ladendiebstähle, Beleidigungen etc. Die damit verbundenen Eingriffe in die Grundrechte der betroffenen Personenkreise stehen in keinem Verhältnis zu den tatsächlichen Möglichkeiten der Polizei, die Begehung der jeweiligen konkreten Straftat zu verhindern. Selbst die Aufklärung begangener, nicht verhinderter Straftaten wird bei massenhafter Speicherung von Daten über vorab "Verdächtige" nicht wesentlich erleichtert. Die bei der Tat gelegten Spuren müssen nämlich einem Verdächtigen zugeordnet werden, was bei steigender Zahl der "Verdächtigen" schwieriger wird. Im Interesse einer effektiven Verhinderung von Straftaten sollte die Datenerhebungsbefugnis in diesen Fällen auf Straftaten mit erheblicher Bedeutung beschränkt werden.

- Das Sächsische Polizeigesetz sollte aus sich selbst heraus verständlich sein und sämtliche Datenverarbeitungsvorgänge seines Regelungsbereiches abschließend normieren. Für den Polizeibeamten muß das Polizeigesetz "sein" Gesetz sein, das er kennt und souverän anwendet; Verweisungen auf allgemeine Vorschriften des Sächsischen Datenschutzgesetzes sind möglich.

- Bei der Erhebung von Daten über Kontakt- und Begleitpersonen zur vorbeugenden Straftatenbekämpfung muß ausgeschlossen sein, daß auch Personen erfaßt werden, die nicht gerade im Hinblick auf die Begehung von Straftaten mit dem potentiellen Straftäter in Kontakt stehen oder ihn begleiten. Deshalb müssen bei Kontakt- und Begleitpersonen tatsächliche Anhaltspunkte dafür bestehen, daß dies der Fall ist.

- Das Bundesverfassungsgericht hat im Volkszählungsurteil auf die besonderen Gefahren der Datenerhebung für das in Art. 8 GG garantierte *Versammlungsrecht* hingewiesen. Datenerhebungen sind somit in diesem Bereich auf die Fälle zu beschränken, in denen sie zum Schutz der Allgemeinheit gemessen am Gewicht des Versammlungsrechts als Grundrecht *verhältnismäßig* sind. Aus diesem Grunde sollte die weitere Aufbewahrung und Nutzung von Daten (zumeist Bildaufzeichnungen), die bei öffentlichen Veranstaltungen oder Ansammlungen erhoben worden sind, von der Erforderlichkeit zur Verfolgung von Straftaten mit

erheblicher Bedeutung abhängig gemacht werden.

- Den gravierendsten Eingriff in das Persönlichkeitsrecht erlaubt der Entwurf des Sächsischen Staatsministerium des Innern, wenn durch *verdeckten Einsatz technischer Mittel* Aufnahmen und Bildaufzeichnungen angefertigt sowie das gesprochene Wort abgehört und aufgezeichnet werden dürfen ("Lauschangriff"), ohne daß der Bereich der Privatwohnung hiervon ausgenommen ist. Ein solcher Lauschangriff greift in den unantastbaren Bereich privater Lebensgestaltung ein und nimmt dem Einzelnen jenen grundgesetzlich geschützten "Innenraum ..., zu dem die Umwelt keinen Zutritt hat" (so das Bundesverfassungsgericht, BVerfGE 27, S. 1, 6) und der obrigkeitlicher - insbesondere heimlicher - Ausforschung entzogen ist. Dies gilt insbesondere auch gegenüber Maßnahmen der Strafverfolgung, die nicht den Wesensgehalt eines Grundrechts, insbesondere das Menschenbild des Grundgesetzes, verletzen dürfen: Eine Wahrheitserforschung um jeden Preis darf es nicht geben.
  Um einen angemessenen Ausgleich zu schaffen zwischen der Aufgabe des Staates, schwerste Straftaten wirkungsvoll zu bekämpfen, und dem Schutzanspruch des Bürgers auf Unverletzlichkeit seines privaten Bereichs, darf ein Lauschangriff zur Straftatenbekämpfung nicht für wirkliche Privatwohnungen im engen Sinn, sondern lediglich für Räume zugelassen werden, die allgemein zugänglich sind oder auch beruflichen oder gesellschaftlichen Tätigkeiten dienen (z. B. Hinterzimmer von Gaststätten, Spielkasinos, Saunaclubs, Bordelle). Unter Berücksichtigung der Interessen der Strafverfolgung sollten allerdings diesen Räumen solche "Wohnungen" gleichgestellt werden, deren Benutzung ersichtlich und ausschließlich Zwecken der Begehung der in einem eng umrissenen Katalog aufgeführten schwersten Straftaten dienen (konspirative Wohnungen). Zu diesem Problem hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 eine Entschließung gefaßt (s.unter Nr. 16.2.6 abgedruckt).
  Die Anordnung des Lauschangriffs wie auch die Anordnung der übrigen "besonderen Mittel der Datenerhebung" wie längerfristige Observation, verdeckter Einsatz technischer Mittel zur Bildaufzeichnung, Einsatz von Vertrauenspersonen und Informanten, Einsatz von Polizeivollzugsbeamten unter Legende (verdeckte Ermittler), muß einem Richtervorbehalt unterliegen. Wird die Maßnahme infolge Gefahr im Verzuge und wegen Nichterreichbarkeit des Richters von dem Behördenleiter oder einem von ihm besonders Beauftragten angeordnet, muß binnen drei Tagen die Anordnung von dem Richter bestätigt werden; wird die richterliche Bestätigung nicht eingeholt, muß die Anordnung außer Kraft treten; für die mittels der Maßnahme bereits erhobenen Daten sollte ein Vernichtungsgebot und ein Verwertungsverbot gelten. Es muß ferner sichergestellt sein, daß durch den Einsatz besonderer Mittel zulässig erhobene Daten einer strengen Zweckbindung unterliegen.

- Das Sächsische Polizeigesetz darf eine *Zweckänderung* von Daten nur zulassen, wenn deren Voraussetzungen im Gesetz klar genannt werden und wenn und soweit der Verhältnismäßigkeitsgrundsatz gewahrt wird. Nicht verfassungsgemäß wäre eine

Vorschrift, die der Polizei gestattet, die Daten jedweder Person, die im Rahmen von Ermittlungsverfahren bekannt geworden sind, zur Wahrnehmung anderer Aufgaben des Polizeivollzugsdienstes und darüber hinaus zur bloßen Dokumentation und zur Vorgangsverwaltung zu speichern, zu verändern oder zu nutzen: Im Rahmen eines Ermittlungsverfahrens werden Daten zumeist vieler Personen bekannt, z. B. Daten von Opfern und Zeugen. Der Zeuge kann z. B. ein Zufallszeuge, das Opfer ein Zufallsopfer sein (z. B. bei Straßenverkehrsdelikten). In diesen Fällen ist es nicht erforderlich, die Daten zur Wahrnehmung vollzugspolizeilicher Aufgaben, insbesondere der vorbeugenden Bekämpfung von Straftaten, zu speichern, es sei denn, es bestünde konkreter Tatverdacht (z.B. in Bezug auf einen fingierten Unfall). Es ist auch nicht angemessen, die Daten aus Strafermittlungsverfahren für jede Aufgabe des Polizeivollzugsdienstes unterschiedslos nutzbar zu machen. Die Zweckänderung sollte nur für die vorbeugende Straftatenbekämpfung zugelassen werden.
Wesentliche Grundlage für die Bewertung der Erforderlichkeit der weiteren Speicherung von Strafverfolgungsdaten zu Zwecken der vorbeugenden Straftatenbekämpfung ist der Ausgang von Strafverfahren. Vor allem Freisprüche, endgültige Verfahrenseinstellungen etc. sind zu berücksichtigen. Die Praxis zeigt, daß häufig diese Informationen nicht zu den Akten gelangen. Deshalb muß das Sächsische Polizeigesetz auch hierfür eine besondere Regelung enthalten.

- Auch muß der *Auskunftanspruch* des Bürgers im Sächsischen Polizeigesetz eine angemessene Ausgestaltung erfahren. Der Auskunftsanspruch kann seine Funktion als verfahrensrechtliche Schutzvorkehrung zur Wahrung des informationellen Selbstbestimmungsrechts, wie sie vom Bundesverfassungsgericht gefordert ist, nur erfüllen, wenn er sich auf den Zweck, die Rechtsgrundlage der Speicherung und vor allem auf die Herkunft der Daten und die eventuellen Empfänger erstreckt. Nur wenn konkrete Versagungsgründe im Einzelfall vorliegen, darf die Auskunft verweigert werden. In diesem Fall wäre es datenschutzrechtlich wünschenswert, wenn die Entscheidung über die Auskunftsverweigerung von der vorgesetzten Behörde zu treffen wäre.
  Die einfache Verweisung auf die allgemeine Auskunftsregelung des § 17 SächsDSG berücksichtigt nicht die Besonderheiten der polizeilichen Datenverarbeitung: Nach § 17 Abs. 3 SächsDSG kann der Betroffene unter Umständen rechtlos gestellt sein, wenn er keine Angaben machen kann, die das einfache Auffinden von Daten ermöglichen. Dem Betroffenen kann jedoch nur auferlegt werden, Angaben zu machen, die in seinen Verantwortungsbereich fallen. Die Verantwortung für das Auffinden von Speicherungen und Akten zur Person des Anfragenden kann nur die ersuchte Behörde tragen. Sie hat ihre Organisation so zu gestalten, daß das Auffinden der Informationen ohne großen Aufwand möglich ist.

Ich werde mich dafür einsetzen, daß alle diese datenschutzrechtlichen Anliegen auf dem weiteren Weg des Entwurfs berücksichtigt werden.

5.10.2 Richtlinien für kriminalpolizeiliche Sammlungen

Das Sächsische Polizeigesetz wird auch den datenschutzrechtlichen Rahmen für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien) vorgeben. Ich begrüße es daher, daß das federführende Landeskriminalamt Sachsen (LKA) mich schon an der Vorbereitung der Richtlinien beteiligt hat. Inzwischen hat das LKA mir zugesichert, meine Empfehlungen weitestgehend zu berücksichtigen.

5.10.3 Polizeiliche Akten in Privatwohnungen

Wie mir ein Petent glaubhaft mitgeteilt hat, wurden seine Person betreffende dienstliche Beschwerdeunterlagen seit Januar 1989 in der Privatwohnung eines sächsischen Polizeibeamten aufbewahrt.

Ich habe diesen Fall zum Anlaß genommen, das Staatsministerium des Innern eindringlich zu bitten, bei der Polizei auf strenge Datensicherung hinzuwirken. Der Landespolizeipräsident hat daraufhin in einer Polizeichefbesprechung die Dienststellenleiter angehalten, der "Einhaltung datenschutzrechtlicher Belange besondere Aufmerksamkeit" zu widmen; ich hätte mir eine konkrete Anweisung gewünscht.

5.10.4 Polizei und private Sicherheitsdienste

Auf private Sicherheitsdienste, deren Betätigung sich insbesondere in den neuen Bundesländern sprunghaft ausgedehnt hat, findet nicht das Sächsische Datenschutzgesetz, sondern das Bundesdatenschutzgesetz (BDSG) mit seinen weitreichenden Datenverarbeitungsbefugnissen Anwendung. Dies darf in der Praxis nicht dazu führen, daß die privaten Sicherheitsdienste die von der Polizei zu beachtenden datenschutzrechtlichen Beschränkungen unterlaufen, soweit sie gleichsam polizeiliche Tätigkeiten ausüben, wie z. B. verdeckte Beobachtungen. Ich halte deshalb besondere gesetzliche Regelungen für die Datenverarbeitung durch private Sicherheitsdienste und Detekteien für dringend erforderlich.
In einem Schreiben an den Staatsminister des Innern habe ich in diesem Zusammenhang auf ein weiteres Problem hingewiesen, nämlich den Datenaustausch zwischen Polizei und privaten Sicherheitsdiensten: Insbesondere in den neuen Bundesländern wird sorgfältig zu überprüfen sein, inwieweit personelle Verflechtungen (Mitarbeiter von privaten Sicherheitsdiensten, die der Volkspolizei oder anderen Sicherheitsorganen der DDR angehört haben) im im verborgenen zu informellen Datenflüssen geführt haben. Aus diesem Grunde beabsichtige ich, noch in diesem Jahr bei der Sächsischen Polizei zu kontrollieren, inwieweit ein Datenaustausch mit privaten Sicherheitsdiensten stattfindet. Der Staatsminister des Innern hat mir hierzu die erforderliche Unterstützung zugesagt.

5.11 Verfassungsschutz

Mit dem Sächsischen Verfassungsschutzgesetz vom 16. Oktober 1992 (GVBl. S. 459) hat der Landtag die rechtliche Grundlage für eine Verfassungsschutzbehörde geschaffen, die im Herbst 1992 ihre Arbeit aufgenommen hat.

Ich versuche, die Bedenken der Bevölkerung gegenüber dem Verfassungsschutz nachvollziehen. Der Staatsicherheitsdienst hat als besonders skrupelloser Geheimdienst die heimliche Ausforschung weiter Bevölkerungskreise betrieben, eine Grauzone von Verdächtigung, Kompromittierung, Ausforschung, Benachteiligung und Staatsverbrechen geschaffen. Dies alles geschah unter grenzenlosem Mißbrauch personenbezogener Daten, heimlich, konspirativ.

Die Aufgaben des Landesamtes für Verfassungsschutz erschöpfen sich jedoch in der *Beobachtung* verfassungsfeindlicher Bestrebungen, sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten für eine fremde Macht, von Bestrebungen, die durch Gewalt die auswärtigen Belange der Bundesrepublik Deutschland gefährden, und auch fortwirkender Strukturen der "Dienste" der DDR, sowie in der *Auswertung* dieser Beobachtungen und entsprechender *Berichterstattung* an die Spitze der Exekutive. Ferner wirkt das Landesamt bei Sicherheitsüberprüfungen mit; dies aber immer mit Wissen des Betroffenen.
Die politische, parlamentarische, gerichtliche und datenschutzrechtliche Kontrolle des Verfassungsschutzes, insbesondere beim Einsatz nachrichtendienstlicher Mittel, ist lückenlos.
Unter den besonderen Bedingungen des jungen Freistaates Sachsen, seiner langen EG-Außengrenze, seiner jüngeren Geschichte und zunehmender Radikalisierung durch linke und rechte Demagogen halte ich die Arbeit des Verfassungsschutzes für notwendig. Die gezogenen Grenzen sind jedoch strikt einzuhalten.
Die nachrichtendienstliche Arbeit des Verfassungsschutzes, das überwiegend heimliche Beschaffen von Informationen, darf dem verfassungsrechtlichen Gebot der Transparenz der Datenverarbeitung nicht zuwider laufen. Deshalb kommt der Präzisierung der Rechtsgrundlagen für Erhebung und Verarbeitung personenbezogener Informationen durch das Landesamt für Verfassungsschutz besondere Bedeutung zu.
Begrüßenswert war, daß der Staatsminister des Innern mir schon in einem frühen Vorbereitungsstadium den Gesetzentwurf zur Stellungnahme vorgelegt hatte. Bereits nach den ersten Erörterungen wurden zahlreiche meiner datenschutzrechtlichen Empfehlungen in den Ressortentwurf eingearbeitet. Die wichtigsten Punkte hierbei waren:

- Die Auskunftserteilung durch das Landesamt für Verfassungsschutz an den Betroffenen wird nicht von dessen Hinweis auf einen konkreten Sachverhalt und von der Darlegung des besonderen Auskunftsinteresses abhängig gemacht. Somit wird der Bürger nicht gezwungen, erst detaillierte Angaben über persönliche Lebensumstände preiszugeben, um Auskunft über die zu seiner Person gespeicherten Daten zu erhalten.

- Die Beteiligung des Sächsischen Datenschutzbeauftragten an der Tätigkeit der Parlamentarischen Kontrollkommission, soweit personenbezogene Daten Gegenstand der Beratungen sind. Dies gewährleistet, was ich für sehr bedeutsam halte, daß die parlamentarische Kontrolle der von großer Eingriffstiefe für das Persönlichkeitsrecht geprägten Verfassungsschutztätigkeit jederzeit über sachverständigen datenschutzrechtlichen Rat verfügt. Im Interesse meiner Unabhängigkeit ist meine Teilnahme an den Sitzungen der PKK auf die konkreten Datenschutzbelange begrenzt.

- Im Rahmen des Minderjährigenschutzes ist eine Speicherung personenbezogener Daten über Personen vor Vollendung des 16. Lebensjahres nicht zulässig.

Im Zuge der parlamentarischen Beratung des Entwurfs der Staatsregierung konnte ich zusätzlich erreichen, daß von einer generalklauselartig erweiterten Aufgabenbestimmung des Landesamtes für Verfassungsschutz Abstand genommen wurde: Der Regierungsentwurf sah vor, daß das Landesamt auch bei "sonstigen Überprüfungen" - also nicht nur bei Sicherheits- und Verfassungstreueüberprüfungen - mitzuwirken hätte. Durch eine solche Regelung wäre das verfassungsmäßige Gebot der Bestimmtheit von Rechtsvorschriften unterlaufen worden: Letzlich hätte die Aufgabenbestimmung des Landesamtes für Verfassungsschutz nicht der hierzu berufene Gesetzgeber, sondern die Exekutive selbst vorgenommen.
Einige meiner datenschutzrechtlichen Empfehlungen fanden dagegen keine Berücksichtigung. So hätte ich es begrüßt, wenn das Verfassungsschutzgesetz die Übermittlung personenbezogener Daten des Landesamtes an andere als öffentliche Stellen (also private Einrichtungen oder Einzelpersonen) nur im Einzelfall erlaubt. Die vom Gesetz eröffnete Möglichkeit des Staatsministers des Innern, eine Zustimmung zur Datenübermittlung "für eine Mehrzahl von gleichartigen Fällen vorweg" zu erteilen, läßt die Gefahr entstehen, nach einem einmal zulässig vorgenommenen Übermittlungsvorgang bei ähnlicher Fallgestaltung später eine vom Gesetz nicht vorgesehene "stillschweigende Übermittlungspraxis" zu begründen.
Eine Erweiterung der Aufgaben des Landesamtes für Verfassungsschutz auf die Beobachtung der "organisierten Kriminalität", wie sie auf Bundesebene diskutiert wird, wäre verfassungswidrig, weil der Freistaat "keinen Geheimdienst mit polizeilichen Befugnissen" unterhält (Art. 83 Abs. 3 S. 1 SächsVerf.).

5.12 Straßenverkehrsbehörden

5.12.1 Bekanntgabe der Entziehung der Fahrerlaubnis an die Polizei

Die Landesbeauftragten für den Datenschutz erörterten das Problem, ob Verwaltungsbehörden die Entziehung von Fahrerlaubnissen bzw. ein ausgesprochenes Fahrverbot der Polizei regelmäßig mitteilen dürfen. Im Ergebnis halten sie eine solche Datenübermittlung für nicht erforderlich und daher für unzulässig. Ich habe mich dieser Ansicht angeschlossen. Die Staatsministerien des Innern sowie für Wirtschaft und Arbeit wurden wie folgt informiert:

Die Übermittlung personenbezogener Daten an öffentliche Stellen ist ohne Kenntnis des Betroffenen gemäß § 4 Abs. 1 i. V. m. § 13 Abs. 1 SächsDSG nur zulässig, wenn ein Gesetz sie erlaubt oder die Datenübermittlung zur Erfüllung der Aufgabe der übermittelnden Stelle oder des Empfängers erforderlich ist. Die Verwendung dieser Daten dient rein polizeilichen Präventivmaßnahmen. Sie ist im Straßenverkehrsrecht ohne konkreten Anfangsverdacht gesetzlich nicht geregelt und daher nicht erlaubt. Die regelmäßige Übermittlung der Daten an die Polizei ist auch nicht erforderlich und widerspricht deshalb dem Grundsatz der Verhältnismäßigkeit. Die Polizei ist im Rahmen der Kontrolle des laufenden und ruhenden Verkehrs bei Verdacht der Begehung einer Ordnungswidrigkeit oder eines Straftatbestandes berechtigt, entsprechende Ermittlungen einzuleiten. Sie kann sich hierzu des Direktzugriffs auf das Verkehrszentralregister in Flensburg bedienen. Vorsorgliche Informationen über entzogene Fahrerlaubnisse bzw. ein Fahrverbot an die Polizei sind daher aus meiner Sicht auch nicht geeignet, die Erfüllung der Aufgaben der Polizei zu verbessern.

Das Staatsministerium des Innern hat inzwischen mitgeteilt, daß die Polizeidienststellen im Freistaat keine regelmäßigen Informationen über den Entzug von Fahrerlaubnissen erhalten.

5.12.2 Datenübermittlung an Medizinisch-psychologische Untersuchungsstellen

Auf Grund einer Eingabe war ich mit der Frage befaßt, ob die nach der Straßenverkehrszulassungsordnung (StVZO) zuständigen Verwaltungsbehörden berechtigt sind, bei Zweifeln hinsichtlich der Eignung eines Führerscheinbewerbers dessen personenbezogene Daten, insbesondere das Führungszeugnis, an Gutachterstellen weiterzuleiten.

Hierzu vertrete ich folgende Auffassung; die ich den Staatsministerien des Innern sowie für Wirtschaft und Arbeit mitgeteilt habe.

Gemäß § 9 StVZO hat die zuständige Verwaltungsbehörde zu ermitteln, ob Bedenken gegen die Eignung des Antragstellers zum Führen von Kraftfahrzeugen vorliegen. Bei dieser Prüfung sind auch schwere oder wiederholte Vergehen gegen Strafgesetze zu berücksichtigen, wie sich aus der beispielhaften Aufzählung in der genannten Vorschrift ergibt. Hat die Verwaltungsbehörde Zweifel, ob ein Bewerber für die Erteilung der Fahrerlaubnis geeignet ist, kann sie gemäß § 12 Abs. 1 StVZO die Beibringung eines Gutachtens einer amtlich anerkannten Medizinisch-psychologischen Untersuchungsstelle fordern. Diese Stellen sind mit Verkehrsmedizinern und Verkehrspsychologen besetzt und arbeiten mit auf die Untersuchung der Verkehrstüchtigkeit ausgerichteten wissenschaftlichen Methoden, wobei auch psychologische Tests verwendet werden dürfen. Aus der Formulierung des Gesetzes, daß die Behörde die Beibringung eines Gutachtens *fordern* kann, ergibt sich, daß es Sache des Bewerbers ist, das Gutachten vorzulegen. Der Bewerber hat daher keinerlei Mitteilungs- oder Offenbarungspflichten, welche Delikte er begangen hat, so daß eine direkte Übermittlung von Führungszeugnissen aus dem Bundeszentralregister und der sonstigen Unterlagen durch die Verwaltung an die Gutachterstelle ohne Einwilligung des Betroffenen nicht zulässig ist.

Die Einwilligung, die üblicherweise auf einem Formular erteilt wird, muß erkennen lassen, welche Verarbeitungsschritte bezogen auf welche Daten erlaubt sein sollen. Weiterhin darf ein Hinweis auf ein Weigerungsrecht des Betroffenen und die Aufklärung über die Folgen der Verweigerung der Einwilligung nicht fehlen (§ 4 Abs. 2 SächsDSG). Außerdem muß die Einwilligungserklärung, die auf den allgemein gebräuchlichen Formularen zusammen mit anderen Erklärungen erteilt wird, im äußeren Erscheinungsbild hervorgehoben sein (§ 4 Abs. 3 SächsDSG). Die im Freistaat von den Führerscheinstellen verwendeten Formulare zur Einverständniserklärung entsprechen nicht den oben genannten Anforderungen.

5.13 Rettungsdienst- und Katastrophenschutzgesetze

Am 21. Januar 1993 ist das Gesetz über Rettungsdienst, Notfallrettung und Krankentransport (SächsRettDG, GVBl. S. 9) in Kraft getreten.

Bereits während der Erarbeitung des Referentenentwurfs beteiligt, konnte ich erreichen, daß das Gesetz mit den Trägern des Rettungsdienstes und den Unternehmern, die die Notfallrettung oder Transporte durchführen, die Adressaten der Datenverarbeitungsvorschrift des § 28 klar benennt. Diese dürfen personenbezogene Daten nur verarbeiten, soweit dies für die Erfüllung ihrer konkret bezeichneten Aufgaben erforderlich ist.

Auch an den Beratungen des Gesetzes über den Katastrophenschutz vom 22. Januar 1993 (SächsKatSG, SächsGVBl. S. 85) bin ich beteiligt gewesen. In dieser schwierigen Materie, bei der Grundrechtseinschränkungen unvermeidbar sind, fanden einige meiner datenschutzrechtlichen Empfehlungen Eingang in den Gesetzestext.

6 Finanzen

Vergleiche unter 5.1.10 und 14.1.1.

7 Kultus

7.1 Datenschutz in der Schule

Das Verhältnis des guten und engagierten Lehrers zu "seinen" Schülern ist geprägt von der Erkenntnis, daß der Mensch aus Leib und Seele besteht. Nicht allein Leistung und Verhalten in einem engen, fachbezogenen Sinn sollen erweckt und gefördert werden, vielmehr ist ein Lehrer häufig Tröster und Freund, Ratgeber und "Sozialarbeiter".

Es wäre aber falsch (und gesetzeswidrig), wenn der Staat dies von oben verordnen und regeln würde. Die Informationen, die Schulleiter und Lehrer für eine individuelle, gerechte und fürsorgliche Ausbildung des einzelnen Kindes benötigen, sind nach Breite und Tiefe sehr unterschiedlich. Sie sind nicht von Amts wegen, sozusagen generell, abzufragen, sondern unterliegen der Verfügungsbefugnis des Kindes und seiner Eltern (Elternrecht). Auch hier darf "der Datenschutz" nicht lebendigen, freiwilligen und persönlichen Kontakt reglementieren oder überhaupt beeinflussen. Soweit es jedoch um Schülerdaten geht, die amtlich und notwendigerweise erhoben, verwendet oder übermittelt werden (müssen), habe ich Regulative vorzuschlagen und gesetzliche Regeln zu überwachen.

Der Unterricht findet nach dem Schulgesetz in einem Schuljahr und in einem Klassenverband (bzw. Kurs) statt: Daten aus früheren Jahren spielen im laufenden Schuljahr keine Rolle; die "Veröffentlichung" aktueller Noten vor der Klasse muß jedoch - nach der pädagogischen Entscheidung des Lehrers - möglich sein. Notenspiegel gehören aber nicht in die Klassenbücher (sie waren in der Vergangenheit häufig Grundlage für die Hackordnung" in manchen Lehrerkollegien), sondern in die Notenbücher des Lehrers selbst, des Fachleiters, des Klassenlehrers und des Schulleiters. Der Schüler und seine Eltern (Sorgeberechtigten) haben einen Anspruch auf Auskunft über die Noten und Erkenntnisse (§ 17 SächsDSG).

Mit dem Kultusministerium habe ich in diesen grundsätzlichen Fragen nach Verhandlungen Einigkeit erzielt.

7.1.1 Verwaltungsvorschrift zum Datenschutz an Schulen

Vom Sächsischen Staatsministerium für Kultus wurde nach Abstimmung mit mir die Verwaltungsvorschrift zum Datenschutz an Schulen und Schulaufsichtsbehörden vom 15. Juli 1992 erlassen, deren Grundlage das Sächsische Datenschutzgesetz ist.

7.1.2 Schulaufnahmeuntersuchungen

Von einer Mutter erhielt ich den Fragebogen, der für die Schulaufnahmeuntersuchung ihres Sohnes auszufüllen war. Es handelt sich um einen als "Anamnese-Ergänzungsbogen" bezeichneten Vordruck aus DDR-Zeiten. Auf meine Nachfrage teilte mir das Landratsamt mit, die Ausfüllung des Bogens sei freiwillig. Das war dem Formular jedoch nicht zu entnehmen und wurde offensichtlich auch von der Mutter nicht so gesehen.

Ich habe das Landratsamt darauf aufmerksam gemacht, daß gemäß § 11 Abs. 2 SächsDSG der Betroffene auf die Freiwilligkeit und nach § 4 Abs. 2 SächsDSG auf das Recht zur Verweigerung der Einwilligung, den Zweck der Datenverarbeitung und die Empfänger einer vorgesehenen Datenübermittlung hingewiesen werden muß.
Aber auch bei Freiwilligkeit dürfen öffentliche Stellen nicht unbeschränkt Daten verarbeiten. Grundsätzlich muß jede Datenverarbeitung für die Erfüllung einer gesetzlichen Aufgabe erforderlich sein. Bei einer freiwilligen Mitwirkung des Betroffenen ist der Maßstab weniger streng. Hier muß die Datenverarbeitung zumindest "förderlich" oder "dienlich" sein. Gleichzeitig sind - sozusagen als Ausgleich - die Formvorschriften über die Einwilligung strikt einzuhalten.
Grundlage der Schulaufnahmeuntersuchung ist § 59 Abs. 5 Schulgesetz (SchulG) in Verbindung mit § 3 Abs. 5 der "Verordnung des Staatsministeriums für Kultus über die Schulgesundheitspflege im Freistaat Sachsen" vom 30. Juni 1992, weiterhin § 27 Abs. 4 und für den Besuch der Förderschule § 30 Abs. 2 SchulG.
Die ärztliche Schulaufnahmeuntersuchung dient gemäß § 3 Abs. 5 der Verordnung zur Feststellung der Schulfähigkeit gemäß § 27 Abs. 4 Satz 2 SchulG aus ärztlicher Sicht. Gemäß § 27 Abs. 4 SchulG können unter anderem ärztliche Untersuchungen durchgeführt werden. Danach kann also von den Eltern verlangt werden, daß sie ihr Kind dem Schularzt vorstellen. Nach dieser Vorschrift können jedoch nicht darüber hinausgehende Auskünfte - mündlich oder schriftlich - gefordert werden. Zudem soll nur festgestellt werden, ob das Kind aktuell den für den Schulbesuch erforderlichen geistigen und körperlichen Entwicklungsstand besitzt. Zu untersuchen ist also der "Ist-Zustand". Daher ergeben sich grundsätzlich Bedenken gegen eine Anamnese, die, wie der Bogen zeigt, sogar in den Bereich einer Sozial- und Familienanamnese hineinreicht. Die Tätigkeit des Schularztes bei der Schulaufnahmeuntersuchung ist also von der eines behandelnden Arztes zu unterscheiden.

Dieses Problem wird seit langer Zeit diskutiert. In Nordrhein-Westfalen haben sich der Landesbeauftragte für den Datenschutz und das Ministerium für Arbeit, Gesundheit und Soziales geeinigt, daß auf die Verwendung von Erhebungsbögen verzichtet werden soll.

Aber selbst dann, wenn man die Verwendung von Anamnese- und anderen Erhebungsbögen akzeptiert, besteht hier eine Reihe von Kritikpunkten, da viele der Angaben nicht einmal dienlich oder förderlich sind. Das gilt für die Frage nach dem Geburtsdatum der Eltern, Tätigkeit, Arbeitsstelle und insbesondere dem Familienstand.

Nicht zulässig ist auch die Frage nach den Geschwistern.
Zwar ist mir bei der Beurteilung medizinischer Fachfragen Zurückhaltung geboten. Dennoch waren bei einigen der medizinischen Angaben Zweifel hinsichtlich ihrer Erforderlichkeit bzw. Förderlichkeit angebracht. Besonders prekär ist die Frage nach Krankheiten anderer Familienmitglieder, weil hier höchst sensible Daten Dritter preisgegeben werden.

Ich habe dem Sächsischen Staatsministerium für Kultus vorgeschlagen, unter Einbeziehung des für den öffentlichen Gesundheitsdienst zuständigen Staatsministeriums für Soziales, Gesundheit und Familie und von Vertretern der Landratsämter gemeinsam eine Lösung zu suchen. Dabei wird auch zur Sprache kommen, daß § 59 Abs. 5 SchulG als Ermächtigung für die Rechtsverordnung über die Schulgesundheitspflege nicht den Anforderungen von Art. 80 Abs. 1 GG, Art. 75 Verfassung des Freistaates Sachsen genügt, da Inhalt, Zweck und Ausmaß der erteilten Ermächtigung nicht hinreichend bestimmt sind. Ebenso entsprechen die §§ 28 Abs. 4, 30 Abs. 2 SchulG, § 3 Abs. 5 der Verordnung nicht den Anforderungen des Bundesverfassungsgerichts (z. B. im Volkszählungsurteil vom 15.12.1983) an die normenklare Regelung des Eingriffs in das Recht auf informationelle Selbstbestimmung. Bereits aus dem Wortlaut eines Gesetzes muß nämlich ablesbar sein, daß und wie weit der Gesetzgeber bewußt und unter Abwägung aller Gesichtspunkte in das Grundrecht auf informationelle Selbstbestimmung zugunsten eines überwiegenden Allgemeininteresses eingreift. Wesentliches Gebot rechtsstaatlicher Normsetzung ist die Vorhersehbarkeit und die Verständlichkeit, im Streitfall auch die richterliche Überprüfbarkeit. Entsprechend ordnet Art. 33 der Verfassung des Freistaat Sachsen an, daß in das Recht des Menschen, über die Erhebung, Verwendung und Weitergabe seiner personenbezogenen Daten selbst zu bestimmen, nur durch oder auf Grund eines Gesetzes - gemeint ist selbstverständlich: einer klar formulierten Rechtsvorschrift - eingegriffen werden darf. Diese Anforderung erfüllen die genannten Vorschriften nicht.
Zu klären sind in diesem Gespräch auch Fragen zu jugendärztlichen Untersuchungen, die nicht als Schulaufnahmeuntersuchungen dienen (§ 3 Abs. 3 der Verordnung).

7.1.3 Aufbewahrung von Unterlagen über Schüler

Der Direktor einer Schule wurde von einem ehemaligen Schüler, der die Schule bereits vor mehreren Jahren verlassen hatte, gebeten, die Unterlagen über ein bestimmtes tragisches Ereignis während seiner Schulzeit herauszugeben. Der Direktor verweigerte dies und bat mich um Rat.

Auch der ehemalige Schüler wandte sich an mich. Für den Fall, daß eine Aushändigung nicht in Betracht komme, wünschte er die Einsichtnahme oder Vernichtung der Unterlagen.

Ich konnte nur die Forderung nach Vernichtung der Unterlagen befürworten.

Für eine Aushändigung bietet nämlich weder das Sächsische Datenschutzgesetz noch die das Gesetz ausfüllende "Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus zum Datenschutz an Schulen und Schulaufsichtsbehörden des Freistaates Sachsen" eine Grundlage.

Auch die bloße Akteneinsicht unterbleibt gemäß § 17 Abs. 5 SächsDSG, wenn die Daten wegen überwiegender Geheimhaltungsinteressen eines Dritten geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Akteneinsicht zurücktreten muß. Nach Prüfung der Unterlagen, die mir im Einverständnis mit dem ehemaligen Schüler überlassen wurden, bin ich zu dem Ergebnis gelangt, daß solche überwiegenden Interessen Dritter im konkreten Fall bestehen.

Es blieb also nur die Möglichkeit einer Vernichtung. Gemäß § 19 Abs. 2 SächsDSG sind personenbezogene Daten in Akten zu löschen, wenn die speichernde Stelle im Einzelfall feststellt, daß die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist. Einschränkungen macht § 19 Abs. 3 SächsDSG, wenn einem Archiv die Unterlagen angeboten werden müssen.
Die Daten über dieses Ereignis waren für die Aufgabenerfüllung nicht mehr erforderlich. Einer Vernichtung stand auch nicht die "Verwaltungsvorschrift des Sächsischen Staatsministeriums für Kultus über die Aufbewahrung und Ausscheidung schulischer Unterlagen" vom 11. September 1992 entgegen. Dort wird eine Aufbewahrungsfrist für Schriftwechsel zwischen dem Schulleiter und dem Kultusministerium, Oberschulamt, staatlichen Schulamt und Schulverwaltungsamt von 15 Jahren angeordnet; diese Vorschrift gilt auch für Unterlagen, die vor ihrem Inkrafttreten entstanden sind. Sie war hier analog anwendbar auf einen Teil der Unterlagen, nämlich auf ein Schreiben des ehemaligen Schuldirektors an den damaligen Kreisschulrat. Die Aufbewahrungsfrist war noch nicht abgelaufen. Dennoch kann diese Verwaltungsvorschrift nicht die nach dem Sächsischen Datenschutzgesetz erforderliche Vernichtung verhindern. Die Aufbewahrungsfristen sind zu rechtfertigen, wenn man in ihnen einen standardisierten Maßstab dafür sieht, wie lange im *Regelfall* Unterlagen "zur Aufgabenerfüllung" im Sinne von § 19 SächsDSG noch erforderlich sind. Hier ergab jedoch die *Einzelfallprüfung*, daß eine längere Aufbewahrung *nicht* gerechtfertigt war. Das bedeutet allerdings noch nicht zwangsläufig die Vernichtung der Unterlagen. Geraten habe ich dem Direktor, zunächst Rücksprache mit dem zuständigen Archiv zu halten, ob nach der noch geltenden Archivordnung der DDR eine Anbietungspflicht besteht. Zudem ist nach der erwähnten Verwaltungsvorschrift bei der Vernichtung von Unterlagen die Schulaufsichtsbehörde zu beteiligen.

Für einen Vermerk des ehemaligen Direktors gilt eine Aufbewahrungsfrist von 5 Jahren, die abgelaufen war, so daß eine Vernichtung unter Beachtung des oben geschilderten Verfahrens erfolgen konnte. Dieselbe Frist gilt für das Protokollbuch, in dem Aufzeichnungen über den Vorfall enthalten waren. Hier besteht jedoch das Problem, daß Akten nur vernichtet werden dürfen, wenn die *gesamte* Akte für die

Aufgabenerfüllung nicht mehr erforderlich ist (§ 19 Abs. 2 SächsDSG). Wenn das Protokollbuch also noch benötigt wird, bleibt nur eine Sperrung der betreffenden Passagen gemäß § 20 Abs. 2 Satz 2 SächsDSG.

7.2 Datenschutz im kirchlichen Bereich

Das Sächsisches Datenschutzgesetz stellt unterschiedliche Anforderungen an die Zulässigkeit einer Datenübermittlung von einer Behörde an eine andere öffentliche Stelle bzw. an einen privaten Empfänger (§§ 13,15). Für die Übermittlung personenbezogener Daten an die öffentlich-rechtlichen Religionsgesellschaften gelten die Regeln über die Übermittlung an öffentliche Stellen (§ 13) entsprechend, sofern für die datenempfangende Religionsgesellschaft "ausreichende Datenschutzregelungen" gelten. Ob das so ist, stellt das Kultusministerium im Einvernehmen mit dem Datenschutzbeauftragten fest (§ 14).
Nach eingehendem Studium der mir vorgelegten kirchlichen Gesetze und Verordnungen der Gliedkirchen der Evangelischen Kirche in Deutschland auf dem Gebiet des Freistaates Sachsen habe ich dem Kultusministerium am 24.1.1992 mitgeteilt, daß dort die geforderten ausreichenden Datenschutzregelungen getroffen sind. Ich verweise auf das Kirchengesetz über den Datenschutz vom 10. November 1977 (ABl.EKD 1978 S. 2), das über Art. 2 § 7 Kirchengesetz des Bundes der Evangelischen Kirche vom 24.Februar 1991 auch in den Gliedkirchen im heutigen Sachsen gilt. Die Kirchen erhalten regelmäßig z. B. Daten über Kirchensteuerpflichtige, Kirchenaustritte und Meldedaten.
Im Rahmen der ihnen verfassungsgemäß (Art. 140 GG, Art. 109 SächsVerf i. V. m. Art. 136 ff. Weimarer Reichsverfassung) zustehenden Autonomie haben die genannten Kirchen einen hohen Datenschutzstandard in ihrem internen Umgang mit personenbezogenen Informationen sichergestellt.

8 Justiz

8.1 Anwendung des Datenschutzgesetzes auf die Tätigkeit der Gerichte und Staatsanwaltschaften

Ein Schreiben des Sächsischen Staatsministeriums der Justiz machte es notwendig, zur Anwendung des Sächsischen Datenschutzgesetzes auf die Tätigkeit der Gerichte grundsätzlich Stellung zu nehmen. § 24 Abs. 2 SächsDSG beschränkt die Kontrollkompetenz des Sächsischen Datenschutzbeauftragten hinsichtlich der Gerichte auf deren Tätigkeit in Justizverwaltungsangelegenheiten. Diese Regelung trägt der durch Art. 97 Grundgesetz verfassungsrechtlich garantierten Unabhängigkeit der Richter Rechnung. Damit soll die *rechtsprechende* Tätigkeit der Gerichte vom Einfluß der anderen des Sächsischen Datenschutzbeauftragten ausgeschlossen ist, weil die in Rede stehende Tätigkeit des Gerichts Rechtsprechungseigenschaft hat.

Dagegen ist für die Auffassung, das Gerichtsprivileg könne auch auf die Staatsanwaltschaften angewandt werden, kein Raum. Staatsanwaltschaftliche Tätigkeit mag zwar in einigen Bereichen auch weisungsfreie Tätigkeit sein, sie ist jedoch gleichwohl keine Rechtsprechung und unterliegt somit der Kontrolle des Sächsischen Datenschutzbeauftragten.

8.2 Informationen an gemeinnützige Empfänger von Bußgeldern

In Sachsen erhalten bei einer Einstellung von Strafverfahren z. B. nach § 153 a StPO die gemeinnützigen Einrichtungen zur Überwachung des Zahlungseingangs Kenntnis von Namen und Anschrift des Betroffenen.

Die Übermittlung von Daten über Personen, gegen die das Verfahren gegen Auferlegung einer Geldzahlung eingestellt wird, durch sächsische Gerichte und Staatsanwaltschaften an private Institutionen hat keine hinreichende gesetzliche Grundlage und ist auch nicht durch eine wirksame Einwilligung der Betroffenen gedeckt. Eine Rechtsgrundlage ist insbesondere weder in der Strafprozeßordnung noch im SächsDSG zu finden:

Nach § 15 Abs. 1 S. 1 SächsDSG dürfen Daten an nicht-öffentliche Stellen nur übermittelt werden, wenn dies zur Erfüllung der Aufgaben der übermittelnden Stelle *erforderlich* ist. Da es der Staatsanwaltschaft bzw. dem Gericht aber durchaus möglich wäre, die Zahlungen der Geldauflagen selbst zu überwachen, ist eine Einschaltung der gemeinnützigen Einrichtung nicht erforderlich. Die Justiz ist ebenso wie die gemeinnützige Einrichtung in der Lage, den Zahlungseingang zu überprüfen. Daß die Überwachung der Geldzahlungen durch die Justiz zusätzliche Personal- und Sachkosten verursachen würde, kann gegenüber der Wahrung des Persönlichkeitsrechts des Beschuldigten nicht ins Gewicht fallen. Im übrigen hätte die Kontrolle der Geldzahlungen durch die Justiz den Vorteil, daß Rückfragen der gemeinnützigen Organisationen bei ausbleibenden Zahlungen vermieden würden und damit eine einfachere Kontrolle des Zahlungseingangs, ohne Zwischenschaltung einer weiteren Stelle, möglich wäre.

Die Datenübermittlung an die gemeinnützigen Einrichtungen ist auch nicht durch eine Einwilligung des Betroffenen gedeckt. Eine wirksame Einwilligung durch den Betroffenen liegt schon deshalb nicht vor, weil es an dem Formerfordernis des § 4 Abs. 3 SächsDSG fehlt. Es ist auch keineswegs davon auszugehen, daß der Beschuldigte mit der Zustimmung zur Einstellung des Verfahrens konkludent (stillschweigend) seine Einwilligung in die Weitergabe seiner Daten an die gemeinnützige Einrichtung erklärt: Adressat seiner Zustimmung ist die Staatsanwaltschaft bzw. das Gericht, Gegenstand seiner Zustimmung ausschließlich die Einstellung des Verfahrens unter Geldauflage. Viele sind mit einer "Verpflichtung zur Geldspende" an eine karitative Einrichtung nur einverstanden, wenn sie selbst (und damit die Verfehlung, für die sie 'büßen müssen')

dabei gegenüber Dritten anonym bleiben.
Ich habe das Sächsische Staatsministerium der Justiz auf die Problematik hingewiesen und gebeten, die Geldzahlungen über die Gerichtskasse abzuwickeln. Eine Übermittlung personenbezogener Daten an gemeinnützige Einrichtungen wäre dann nicht erforderlich. Anfang April 1993 werde ich mit dem Staatsministerium die weitere Verfahrensgestaltung besprechen.

8.3 Protokollierung der Einsichtnahme in das Grundbuch

Das Berliner Abgeordnetenhaus hat im Berliner Ausführungsgesetz zum Gerichtsverfassungsgesetz eine Regelung getroffen, die dem Anliegen des Datenschutzes in umfassender Weise genügt. Insbesondere sollen alle Fälle, in denen jemand das Grundbuch einsieht, protokolliert werden.

Aus meiner Sicht ist es wünschenswert, daß auch für Sachsen eine entsprechende Regelung geschaffen wird. Das Grundbuch soll keine Hilfe sein, Interessantes zu erfahren, sondern ein Instrument des Rechtsverkehrs. § 12 Grundbuchordnung (GBO) wägt sachgerecht zwischen dem Interesse an der Einsichtnahme in das Grundbuch und dem Schutz des Persönlichkeitsrechts des Einzelnen ab. Nach dieser Vorschrift kann jeder Einsicht in das Grundbuch nehmen, wenn er ein berechtigtes Interesse darlegt. Nur in diesem Fall geht die Publizität des Grundbuchs dem Persönlichkeitsrecht des im Grundbuch Eingetragenen vor, sei er nun Eigentümer oder sonstiger eingetragener Berechtigter. Dessen Recht auf informationelle Selbstbestimmung wird verletzt, wenn einem Dritten Einsicht gewährt wird, ohne daß dieser ein berechtigtes Interesse dargelegt hat. Der Betroffene kann die Entscheidung des Grundbuchamts, die Einsicht im Grundbuch zu gewähren, auch nachprüfen lassen. Auch wenn er hierdurch die bereits erfolgte Einsichtnahme nicht mehr verhindern kann, ist die präventive Wirkung einer Protokollierungspflicht nicht zu unterschätzen.

Um das Kontrollrecht der von der Einsichtnahme Betroffenen zu stärken, sollte außer dem Namen der Einsichtnehmenden auch der Grund für die Einsichtnahme, zumindest stichwortartig, angegeben werden. Damit auf der anderen Seite das Persönlichkeitsrecht der Einsichtnehmenden besser geschützt wird, sollte ein Urkundsbeamter in einem gesonderten Heft und nicht der Einsichtnehmende selber dies protokollieren. Nur so kann verhindert werden, daß der Einsichtnehmende Kenntnis von den anderen Personen erlangt, die vor ihm Einsicht in das Grundbuch genommen haben.
Beim Sächsischen Staatsministerium der Justiz habe ich eine entsprechende Regelung für Sachsen angeregt.

8.4 Aufbewahrungsbestimmungen

Nach Abschnitt 1 Nrn. 4 u. 602, der "Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden" (Aufbewahrungsbestimmungen) i. V. m. § 7 Abs. 8 Aktenordnung (AktO) soll die für eine Akte angelegte Karteikarte dann weggelegt werden, wenn der Aktenvorgang ausgeschieden worden ist. Im folgenden Jahr nach der "Weglegung" der Karteikarte beginnt dann die Aufbewahrungsfrist von fünf Jahren. Die Karteikarten werden also sechs Jahre länger als der dazugehörige Aktenvorgang aufbewahrt.

Die Aufbewahrungsbestimmungen sind Verwaltungsvorschriften. Sie sind auf Grund eines (schon länger zurückliegenden) Beschlusses der Konferenz der Justizverwaltungen des Bundes und der (alten) Länder inhaltlich gleichlautend durch Erlasse der einzelnen Landesjustizverwaltungen in Geltung gesetzt worden. Einen solchen Erlaß gibt es in Sachsen zwar bisher nicht; die Aufbewahrungsbestimmungen und die AktO werden gleichwohl angewandt.

Aus datenschutzrechtlicher Sicht ist diese Verfahrensweise nicht haltbar:
Die Aufbewahrungsbestimmungen stellen keine ausreichende Rechtsgrundlage i. S. v. § 4 Abs. 1 Nr. 1 SächsDSG für die Aufbewahrung (Speicherung nach § 3 Abs. 2 Nr. 2 SächsDSG) derjenigen personenbezogenen Daten dar, die in den Karteikarten (Dateien i. S. v. § 3 Abs. 5 S. 2 SächsDSG) enthalten sind. Da § 4 Abs. 1 Nr. 1 SächsDSG nur eine Ausprägung des Grundsatzes des *Vorbehalts des Gesetzes* ist, sind unter Rechtsvorschriften - der üblichen Terminologie folgend - nur Gesetze im formellen Sinne bzw. durch förmliches Gesetz gedeckte Rechtsverordnungen oder Satzungen zu verstehen, nicht jedoch bloße verwaltungsinterne Regeln, wie Erlasse, Verwaltungsanweisungen, Dienstvorschriften etc.

Die Aufbewahrung der Karteikarten ist auch nicht durch § 12 SächsDSG erlaubt. Danach ist das Speichern personenbezogener Daten zulässig, wenn dies, neben weiteren Voraussetzungen, zur Erfüllung der gesetzlichen Aufgaben der öffentlichen Stelle erforderlich ist. Es ist nicht ersichtlich, welchem Zweck die Karteikarten noch dienen, wenn die dazugehörigen Akten schon vernichtet sind. Da es in Sachsen noch keine Karteikarten geben dürfte, ohne daß auch entsprechende Akten dazu bestünden, sollte bereits jetzt dem Entstehen einer solchen Situation entgegengewirkt werden. ´

Mit einem Schreiben dieses Inhalts habe ich mich an das Sächsische Staatsministerium der Justiz gewandt.

Die sehr komplizierten, weil unübersichtlichen und jede Aktenart gesondert behandelnden Aufbewahrungsbestimmungen für Justizakten müssen entrümpelt, d.h. radikal vereinfacht werden.

8.5 Automation in der Geschäftsstelle einer Staatsanwaltschaft

Erst anläßlich der Sitzung des Arbeitskreises Justiz der Datenschutzbeauftragten des Bundes und der Länder am 24. Juni 1992 in München habe ich durch einen Vertreter des Bayerischen Staatsministeriums der Justiz erfahren, daß bei der Staatsanwaltschaft bei dem Landgericht Dresden - als bislang einziger Staatsanwaltschaft in Sachsen - ein automatisiertes Aktenverwaltungssystem (SIJUS-straf) eingesetzt wird.

Bei meiner daraufhin dort durchgeführten Kontrolle stellte ich fest, daß in dem in Dresden zunächst im Probebetrieb laufenden, in Bayern bereits im Echtbetrieb eingesetzten Verfahren bisher von Hand in Karteikarten, Loseblatt- oder Buchform erfaßte personenbezogene Daten in großem Umfang gespeichert werden.

Zutage traten hierbei Probleme der Datensicherung nach § 9 Abs. 2 SächsDSG, insbesondere der Zugangs-, Speicher- und Zugriffskontrolle, die zum Teil durch die unzureichende Raumsituation im Dresdner Justizgebäude bedingt waren.

Wie mir der Leitende Oberstaatsanwalt beim Landgericht Dresden kürzlich mitgeteilt hat, wird das automatisierte Verfahren fortgeführt. Über inzwischen vorgenommene Verbesserungen der Datensicherheit werde ich mich noch in diesem Jahr unterrichten.

Zur Thematik ist allgemein anzumerken, daß für die Verarbeitung personenbezogener Daten durch die Geschäftsstellen der Justiz keine rechtlichen Grundlagen von ausreichender Normqualität bestehen. Die bundeseinheitliche Verwaltungsvorschrift "Aktenordnung für die Geschäftsstellen der Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften (AktO)", an der sich auch das vorliegende Verfahren orientiert, sollte durch ein bereichsspezifisches Gesetz ersetzt werden. Zu diesem Regelungsbereich des Strafrechts liegt seit 1989 ein Referentenentwurf eines Strafverfahrensänderungsgesetzes vor.

8.6 Pilotprojekt Täter-Opfer-Ausgleich

Das Sächsische Staatsministerium der Justiz regte im Jahre 1992 ein "Pilotprojekt Täter-Opfer-Ausgleich für den Bereich Dresden" an, um zu erproben, ob für den Kreis jugendlicher und erwachsener Straftäter ein konfliktschlichtender Täter-Opfer-Ausgleich geeignet ist, spezialpräventive (erzieherische) Wirkung zu erzielen, wirksame und schnelle Befriedigung der Ansprüche der Verletzten zu erreichen und die Anzahl der Gerichtsverfahren zu reduzieren.

Die Streitschlichtung, wie sie in diesem Projekt vorgesehen ist, wird eingeleitet, wenn die Staatsanwaltschaft einen Vorgang hierfür geeignet hält. Anschließend werden erst das Opfer, dann der Täter gefragt, ob sie mit einer Streitschlichtung einverstanden sind. Falls beide das bejahen, schickt die Staatsanwaltschaft die Akten an die Konfliktschlichtungsstelle. In dem dann stattfindenden Schlichtungsverfahren sollen die Interessen des Opfers, z. B. die Erwartung eines Schadensausgleichs, berücksichtigt

und der in der Tat zu Tage getretene Konflikt zwischen Täter und Opfer erforscht, besprochen und nach Möglichkeit abgebaut werden. Der übliche Strafprozeß leistet dies alles nur ungenügend; in ihm geht es um Bestrafung, d.h. um Sühne, und, vielfach nur unzureichend, um Resozialisierung des Täters.

Aus datenschutzrechtlicher Sicht bestehen gegen dieses Vorhaben keine grundsätzlichen Bedenken, weil die Streitschlichtung nur stattfindet, wenn Opfer und Täter damit einverstanden sind. Das ist erforderlich, weil eine gesetzliche Grundlage für den Datenaustausch - hier ist der Bundesgesetzgeber zuständig - noch fehlt.
Bei der Einholung des Einverständnisses wird zu beachten sein, daß sowohl Täter als auch Opfer schriftlich umfassend über die Folgen ihrer Einverständniserklärung aufgeklärt werden. Das Einverständnis sollte ebenfalls schriftlich erklärt werden. Schließlich muß den Betroffenen in jedem Fall mitgeteilt werden, warum und wer im einzelnen ihre personenbezogenen Daten erhält. Weiterhin sollten sie schriftlich auf ihr Recht zur Verweigerung der Einwilligung hingewiesen werden. § 4 SächsDSG ist zu beachten.

Meine Gespräche haben folgendes ergeben:
Das Sächsische Staatsministerium der Justiz wird den Trägerverein des Pilotprojekts (Verein zur Förderung der sozialen Rechtspflege Dresden e. V.) darauf hinweisen, daß für ihn, da er öffentliche Aufgaben wahrnimmt, das Sächsische Datenschutzgesetz gilt. Weiterhin wird das Sächsische Staatsministerium der Justiz per Runderlaß die Staatsanwaltschaften auf die Geltung des Verhältnismäßigkeitsgrundsatzes bei der Versendung von Akten an die Konfliktschlichtungsstelle hinweisen. Aktenbestandteile, die weder die Täter- noch die Opferpersönlichkeit, wohl aber Dritte betreffen, sollen mangels Erforderlichkeit nicht an die Schlichtungsstelle übersandt werden. Schließlich wird das Sächsische Staatsministerium der Justiz prüfen, ob Regelungen über Datenübermittlungen im Rahmen der Arbeit der Schlichtungsstelle im Justizmitteilungsgesetz Aufnahme finden können.

Ich freue mich über die gute Zusammenarbeit in diesen Fragen.

9 Wirtschaft und Arbeit

9.1 Gewerberecht

9.1.1 Rechtliche Entwicklung

In der Gewerbeordnung fehlen bislang bereichsspezifische Regelungen für die Erhebung und die Übermittlung von Daten. Der Bundesgesetzgeber beabsichtigt jedoch, entsprechende Bestimmungen in das Gesetz aufzunehmen. So sollen u. a. in einem künftigen § 14 der Gewerbeordnung (GewO) detailliert die Voraussetzungen für Datenübermittlungen an Behörden und Gewerbeauskünfte an Private - allerdings nach

meinem Dafürhalten unbefriedigend - geregelt werden.

In meiner Stellungnahme zu dem Gesetzentwurf habe ich wie folgt argumentiert:
§ 14 Abs. 8 GewO-Änderungsentwurf regelt die regelmäßige und fallweise einfache und erweiterte Gewerbeauskunft an den nichtöffentlichen Bereich. Auch Gruppenauskünfte sollen sich (laut Gesetzesbegründung) nach dieser Vorschrift beurteilen. In Analogie zum Melderecht halte ich Regelungen über die Voraussetzungen von Gruppenauskünften (Vorliegen eines öffentlichen Interesses) für geboten. Der Bayerische Landesbeauftragte für den Datenschutz hat in seinem 10. Tätigkeitsbericht in Nr. 7.8.2 auf die Diskrepanz hingewiesen, die sich bei Adreßbuchverlagen erteilten Gruppenauskünften ergibt, je nach dem, ob die Auskunft aus dem Melderegister oder aus der Gewerbekartei geschieht. Die im Melderecht bestehende Widerspruchsmöglichkeit sollte deshalb auch in der GewO vorgesehen werden.

Andererseits scheint mir das Erfordernis des "berechtigten Interesses" bei einfachen Gewerbeauskünften und des "rechtlichen Interesses" bei erweiterten Gewerbeauskünften überzogen. Ich halte es - wie der Bayerische Landesbeauftragte für den Datenschutz in seinem 14. Tätigkeitsbericht - für vertretbar und angemessen, wenn *einfache* Gewerbeauskünfte, ähnlich wie im Melderecht, von der Gewerbebehörde *ohne* Bedingungen erteilt werden.
Für *erweiterte* Gewerbeauskünfte müßte es genügen, wenn der Auskunftssuchende anstelle eines *rechtlichen* Interesses nur ein *berechtigtes* Interesse glaubhaft macht, wobei unter *berechtigtem* Interesse jedes von der Rechtsordnung geschützte, insbesondere auch ein wirtschaftliches Interesse, zu verstehen ist. Auch die Verpflichtung, den Gewerbetreibenden über eine erteilte erweiterte Auskunft zu benachrichtigen (welche Daten an welchen Empfänger), sollte geregelt werden. Ich habe beim Bundesbeauftragten für den Datenschutz angeregt, meine Stellungnahme dem Bundeswirtschaftsministerium zur Berücksichtigung im Gesetzgebungsverfahren vorzulegen.

9.1.2 Gewerbeauskünfte - Verfahrensweise im Freistaat Sachsen

Bis zum Inkrafttreten der bereichsspezifischen Bestimmungen über Gewerbeauskünfte in der Gewerbeordnung richtet sich die Erteilung von Auskünften nach dem Sächsischen Datenschutzgesetz.

Deshalb hat mich das Staatsministerium für Wirtschaft und Arbeit gebeten, das Gewerbeauskunftsverfahren aus datenschutzrechtlicher Sicht zu würdigen. Ich habe im vorstehend dargelegten Sinne Stellung genommen.
Die daraufhin vom Ministerium erlassene "Richtlinie über die Behandlung von Anzeigen nach §§ 14 und 55 c Gewerbeordnung" vom 21. Dezember 1992 (SächsABl 1993, S. 44) enthält die nach meinem Dafürhalten, wie dargelegt, überzogene Forderung, *einfache* Gewerbeauskünfte grundsätzlich vom Vorliegen eines *berechtigten* Interesses und *erweiterte* Gewerbeauskünfte vom Vorliegen eines

rechtlichen Interesses abhängig zu machen. Außerdem ist der Betroffene nach derzeitiger Rechtslage gemäß § 15 Abs. 3 SächsDSG *vor* der Erteilung erweiterter Auskünfte zu hören *und danach* über die erteilte erweiterte Auskunft zu benachrichtigen (wer hat welche Daten erhoben).
Die Anwendbarkeit der-eben nicht-bereichsspezifischen, subsidiären Regelung des SächsDSG erzwingt diese nachmeinem Dafürhalten, wie dargelegt, in der Sache überzogenen Anforderungen. Ich hoffe deshalb, daß der Bundesgesetzgeber meinen Vorschlägen folgt und das Gewerbeauskunftsverfahren in der Gewerbeordnung mit Augenmaß regelt.

9.2 Offene Vermögensfragen

9.2.1 Rechtliche Entwicklung

Die Klärung der sog. offenen Vermögensfragen, ausgehend von der Gemeinsamen Erklärung der beiden deutschen Regierungen vom 15. Juni 1990, gehört zu den dringendsten und schwierigsten Aufgaben, die sich im Zusammenhang mit der Wiederherstellung der staatlichen Einheit Deutschlands stellen. Die dafür geschaffenen maßgebenden rechtlichen Regelungen, vor allem das "Gesetz zur Regelung offener Vermögensfragen" (VermG), sind vom Gesetzgeber in kurzen Zeitabständen geändert und ergänzt worden. Verwaltungspraxis und Rechtsprechung haben sich noch nicht festigen können. Zu den rein rechtlichen Schwierigkeiten kommen solche der Tatsachenfeststellung: Es müssen von den dafür zuständigen 'Vermögensämtern' (Ämter oder Landesämter zur Regelung offener Vermögensfragen) Sachverhalte ermittelt werden, die zum Teil Jahrzehnte zurückliegen.

Mit den Rechtsänderungen, die das Zweite Vermögensrechtsänderungsgesetz vom 14. Juli 1992 gebracht hat, ist eine Beschleunigung der Klärung der offenen Vermögensfragen und eine Erleichterung von Investitionen bezweckt worden. In diesem Zusammenhang wurde auch eine besondere datenschutzrechtliche Vorschrift eingefügt: Es besteht ein erhebliches öffentliches Interesse daran, daß Verwaltungsverfahren nach dem Vermögensgesetz durch unmittelbare Einigung unter den Beteiligten, einschließlich investitionswilliger Dritter, erledigt werden (vgl. auch § 31 Abs. 5 VermG), so daß ein Verwaltungsverfahren nach dem Investitionsvorranggesetz gar nicht mehr nötig wird. Im Hinblick darauf gibt § 32 Abs. 5 VermG den Vermögensämtern die datenschutzrechtlich abgesicherte Möglichkeit, "Namen und Anschriften der Antragsteller" sowie den "Vermögenswert", auf den sich der Antrag bezieht, einem Dritten mitzuteilen, wenn dieser "ein berechtigtes Interesse" daran "glaubhaft" macht und wenn der Antragsteller nach vorheriger diesbezüglicher Unterrichtung einer solchen Daten-Weitergabe nicht wiedersprochen hat.

Die Überprüfung, ob im Einzelfall ein Vermögensamt **unter Verstoß** gegen § 35 Abs. 5 VermG Daten weitergegeben hat, hat der Gesetzgeber allerdings bedauerlicherweise dadurch sehr erschwert, daß er für diese Weitergabe nicht die Schriftform vorgeschrieben hat.

9.2.2 Anwendbarkeit des § 32 Abs. 5 VermG auf Auskunftsersuchen von Finanzbehörden?

Im Hinblick auf die zuletzt genannte Vorschrift hat mich das Sächsische Landesamt zur Regelung offener Vermögensfragen um Stellungnahme zu der Frage gebeten, ob § 32 Abs. 5 VermG ein Recht des Antragstellers begründet, einer Auskunftserteilung des Vermögensamtes zu widersprechen, durch welche dieses auf entsprechendes Ersuchen seine Amtshilfepflichten gemäß §§ 111, 112 Abgabenordnung (AO) gegenüber den Finanzbehörden erfüllte; ob also ein Widerspruchsrecht bestehe und vor der Auskunftserteilung an die Finanzbehörde der Antragsteller auf dieses Recht hinzuweisen sei.

Dazu habe ich die Auffassung vertreten, daß § 32 Abs. 5 VermG mit seinem Erfordernis einer Darlegung eines 'berechtigten Interesses' *nicht* auf die Fälle gesetzlich geregelter *Verpflichtung* zur Auskunftserteilung (im Wege der Amtshilfe) zugeschnitten ist. Mit anderen Worten: Auskünfte, die auf Grund gesetzlicher Vorschriften erteilt werden müssen, fallen nicht in den Regelungsbereich des § 32 Abs. 5 VermG, so daß diese Vorschrift *insoweit* ein Widerspruchsrecht, auf das hinzuweisen wäre, *nicht* begründet.
Ich habe jedoch angeregt, nichtsdestoweniger die Antragsteller in geeigneter Form von der Datenweitergabe an die Finanzämter zu unterrichten.

9.2.3 Datenweitergabe an Immobilienunternehmen

Mehrere Eingaben und Presseberichte veranlaßten mich, der Frage nachzugehen, ob in einzelnen Fällen im Bereich der Klärung offener Vermögensfragen tätige öffentliche Stellen Daten von Antragstellern ohne deren Einverständnis an Unternehmen der Grundstückswirtschaft weitergegeben haben.

Die befragten Unternehmen gaben an, die Daten durch eigene Nachforschungen ermittelt zu haben und nicht mehr feststellen zu können, woher bestimmte Informationen stammen.

Angesichts dessen sind diese Unternehmen, die als nicht-öffentliche Stellen nicht in meinen Zuständigkeitsbereich fallen, auf § 34 BDSG hinzuweisen, der auch private Stellen verpflichtet, einem Betroffenen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen - einschließlich der Angabe, woher diese stammen. Außerdem scheint mir § 28 Abs. 1 BDSG einschlägig zu sein, wonach Daten nur "nach Treu und Glauben und auf rechtmäßige Weise erhoben werden" dürfen.

Es liegt nahe, daß die Unternehmen in diesen Fällen die Daten von öffentlichen Stellen erhalten haben. Ich konnte das aber nicht nachweisen. Der Verdacht konnte allerdings auch nicht ausgeräumt werden. Datenhandel ist schließlich ein einträgliches Geschäft. - Ich werde die Szene beobachten.

9.2.4 Anforderung von Grundbuchauszügen durch die Grundstücksverkehrsgenehmigungs-Behörde

Ein Landratsamt hat im Genehmigungsverfahren nach der Grundstücksverkehrsordnung (GVO, in der Fassung des Art. 4 des 2. VermögensrechtsänderungsG) von den Antragstellern die Vorlage von Grundbuchauszügen verlangt.
Ich habe der Behörde mitgeteilt, daß dies datenschutzrechtlich unzulässig ist, weil die Kenntnisnahme des Grundbuch-Inhaltes durch die Behörde für die Überprüfung der Genehmigungsfähigkeit eines Grundstücks-Kaufvertrages *nicht* erforderlich ist.
Nach § 1 GVO ist nämlich die Erteilung der Genehmigung davon abhängig, ob für das betreffende Grundstück ein Rückübertragungsanspruch angemeldet ist. Um das zu überprüfen, benötigt die Behörde aber lediglich die genaue Bezeichnung des Grundstückes, welches Gegenstand des Kaufvertrages ist. Diese wiederum muß aus sachen- bzw. grundbuchrechtlichen Gründen ohnehin aus dem zur Genehmigung vorgelegten Vertrag hervorgehen! Die Eigentums- und ggf. sonstigen Rechtsverhältnisse an dem Grundstück, wie sie sich aus dem Grundbuchauszug ergeben, sind demgegenüber für das Verwaltungsverfahren unerheblich.

9.3 Clearingstelle beim Sächsischen Wirtschaftsministerium

Beim Sächsischen Staatsministerium für Wirtschaft und Arbeit (SMWA) ist eine "Clearingstelle" eingerichtet worden, deren Aufgabe es ist, Beschwerden über Personen zu sammeln, die "sich *dem wirtschaftlichen Neuaufbau in den Weg stellen*". Diese Stelle leitet Informationen aus der Bevölkerung, von Seiten der Betriebsräte, aus den Betrieben und Gewerkschaften an die Treuhandanstalt weiter. Presseveröffentlichungen (z. B. Dresdner Neueste Nachrichten vom 4.8.1992) sowie eine Kleine Anfrage der SPD (LTDrs. 1/2015) und deren Beantwortung habe ich zum Anlaß genommen, die datenschutzrechtliche Seite zu prüfen.

Ich habe folgendes festgestellt:

1. Entgegen der Pressedarstellung und der Antwort auf die Kleine Anfrage werden Beschwerden an Stellen der Staatsregierung, an die Regierungspräsidien oder an andere Stellen nur in den wenigen Fällen weitergegeben, in denen das SMWA ganz offensichtlich der falsche Adressat war.

2. Bei jedem Ministerium, jeder größeren Behörde in den neuen Bundesländern gehen viele Eingaben und Beschwerden von Bürgern ein. Damit wird eine gewisse Tradition, die typisch für die DDR war, fortgesetzt: Da gerichtlicher Schutz kaum zu erreichen und zu erwarten war, haben sich die Bürger lieber -und in großer Zahl- mit Eingaben an hochrangige Dienststellen gewandt.
   Diese Eingaben müssen bearbeitet werden. Denn jeder hat Anspruch auf eine angemessene Antwort, wenn er sich an eine Behörde wendet. Die Sächsische Verfassung regelt, in ihrem Grundrechtsteil in Art. 35, daß sich jede Person mit

Bitten und Beschwerden an die zuständigen Stellen wenden kann und daß ein Anspruch auf begründeten Bescheid in angemessener Frist besteht. Wenn das SMWA eine eigene Stelle zur Bearbeitung dieser Vorgänge einrichtet, so hält sich dies im Rahmen der Organisationshoheit des Ressorts.

3. Weitere Rechtsgrundlage der Tätigkeit des SMWA und der von diesem veranlaßten Tätigkeit der Treuhandanstalt ist das Treuhandgesetz. Nach § 2 Treuhandgesetz hat sie als Anstalt des öffentlichen Rechts der Privatisierung und Verwertung volkseigenen Vermögens nach den Prinzipien der sozialen Marktwirtschaft zu dienen. Gemäß § 2 Abs. 6 Treuhandgesetz hat die Treuhandanstalt ferner die Strukturanpassung der Wirtschaft an die Erfordernisse des Marktes zu fördern, indem sie insbesondere auf die Entwicklung sanierungsfähiger Betriebe zu wettbewerbsfähigen Unternehmen und deren Privatisierung Einfluß nimmt. Sie wirkt darauf hin, daß sich durch zweckmäßige Entflechtung von Unternehmensstrukturen marktfähige Unternehmen herausbilden und eine effiziente Wirtschaftsstruktur entsteht.

   Da die Treuhandanstalt gemäß § 1 Abs. 4 Treuhandgesetz Inhaber der Anteile aller ehemaligen volkseigenen Betriebe ist, soweit diese nicht bereits privatisiert sind, ist sie wirtschaftlich gesehen (juristisch nur mittelbar) Arbeitgeber sämtlicher in diesen Betrieben Beschäftigten. Als solcher ist sie zuständig für die Entgegennahme und Auswertung der über das SMWA an sie herangetragenen Beschwerden und Anregungen, welche die noch nicht privatisierten Unternehmen und deren Beschäftigte betreffen. Das SMWA seinerseits ist im Rahmen seiner Obliegenheit, die sächsische Wirtschaft zu fördern, zuständig und berechtigt, diese Beschwerden und Anregungen entgegenzunehmen und dorthin weiterzugeben, wo die rechtliche Möglichkeit besteht, auf Grund von Beschwerden Maßnahmen zu treffen, eben an die Treuhandanstalt.

4. Das SMWA hat die "Clearingstelle" ordnungsgemäß organisiert und die notwendigen Datenschutz- und Sicherheitsanforderungen erfüllt: Auslagerung, sorgfältige Auswahl und Verpflichtung der Mitarbeiter, Ausschaltung des allgemeinen Schreibdienstes; die Zusicherung von Vertraulichkeit auf besonderen Wunsch der Petenten wird strikt eingehalten.

Aus den genannten Gründen ist die wichtige Arbeit der Clearingstelle datenschutzrechtlich nicht zu beanstanden; sie ist zur Erledigung der gesetzlichen Aufgaben des Ministeriums und der Treuhandanstalt erforderlich.

Datenübermittlungen an Regierungspräsidien und "zuständige Stellen in der Staatsregierung" finden - nur ganz ausnahmsweise - lediglich dann statt, wenn die Beschwerden und Anregungen nicht (Privat-)Betriebe, sondern Mitarbeiter von Behörden oder nachgeordneten Dienststellen (z. B. Forschungsinstitute) betreffen. Die Unterlagen des Petenten werden in diesen Fällen nach Zuständigkeitsgesichtspunkten verteilt. Auch dagegen ist aus datenschutzrechtlicher Sicht nichts einzuwenden.

10 Soziales und Gesundheit

10.1 Gesundheitswesen

10.1.1Krankenhausgesetz

Zu den bedeutendsten Vorhaben im Gesundheitswesen zählte der Entwurf des Gesetzes zur Neuordnung des Krankenhauswesens im Freistaat Sachsen (Sächsisches Krankenhausgesetz). Er enthält in § 35 Regelungen zum Datenschutz, zu denen ich ausführlich Stellung genommen habe. Im wesentlichen sind sie zu begrüßen. Ein erhebliches Defizit besteht allerdings darin, daß die für die Praxis besonders wichtige Regelung von Forschungsvorhaben fehlt.

10.1.2 Krebsregistergesetz

Von Beginn meiner Tätigkeit an habe ich ganz besondere Aufmerksamkeit den Problemen eines Krebsregisters gewidmet. In der DDR bestand in Berlin (Ost) ein "Nationales Krebsregister", das ein Einzugsgebiet von 16,5 Millionen Einwohnern umfaßte. Im Zeitpunkt der Wiedervereinigung wurde ein Datenbestand von ca. 2,2 Mio Fällen betreut. Auf vollständige Datensätze kann beim Krebsregister bis zum Jahr 1961 zurückgegriffen werden.

Die Pflicht aller Ärzte der DDR, Geschwulsterkrankungen zu melden, wurde 1953 eingeführt. Jede Verdachtsdiagnose, jedes Rezidiv (Wiederauftreten) und jede Metastasierung sowie jeder Todesfall eines Krebskranken war dann von der zuständigen Betreuungsstelle für Geschwulsterkrankungen zu melden, von denen rund 200 im Gebiet der DDR bestanden. Die Meldungen bildeten die Arbeitsgrundlage für die Betreuung der Patienten. An Hand spezieller Meldebögen war das Krebsregister zu unterrichten. Dort wurden die Daten gesammelt, gespeichert und verarbeitet. Weder für die Datenerhebung noch für das Speichern oder Übermitteln dieser besonders sensiblen Daten war eine Einwilligung der betroffenen Personen erforderlich. Rechtsgrundlage für die Datenerhebung stellte die Verordnung zur Verbesserung der Behandlung von Geschwulsterkrankungen vom 17. Mai 1956 (GBl. I Nr. 54 S. 477) dar. Durch das Statistikgesetz der DDR vom 17. August 1990 wurde bestimmt, daß die amtlichen Statistiken durch Gesetze angeordnet werden. Dabei ist auch die Erhebung "Nationales Krebsregister" als amtliche Statistik angeordnet worden.

Da das Statistikgesetz im Einigungsvertrag nicht als weitergeltendes Recht der DDR aufgeführt ist, war seit dem 3. Oktober 1990 eine gesetzliche Regelung erforderlich geworden, um die im Krebsregister gespeicherten Daten vor unbefugten Zugriff zu sichern sowie eine datenschutzgerechte Auswertung zu ermöglichen. Ohne eine gesetzliche Grundlage drohte sogar eine Löschung, da die Daten - ohne Einwilligung! –

rechtswidrig erhoben worden waren. Damit wären wertvolle Daten, deren Anonymisierung technisch möglich wäre, für die Wissenschaft und die Gesundheitspolitik verloren gegangen. Im internationalen Vergleich der bevölkerungsbezogenen Krebsregister ist das Krebsregister der ehemaligen DDR das mit der größten zugrundeliegenden Population.
Der Wissenschaftsrat hat in seiner Stellungnahme zu den außeruniversitären Forschungseinrichtungen in der ehemaligen DDR gefordert, eine Rechtsgrundlage zu schaffen, um den Datenbestand zu sichern und eine lückenlose weitere Datenerhebung zu ermöglichen. Er hat festgestellt, daß entscheidende Voraussetzung für eine vorbeugende Krebsbekämpfung und die Bewertung präventiver und kurativer Maßnahmen verläßliche Angaben über Auftreten und Art von Krebserkrankungen in Beziehung zu ihrer Umwelt sind. Diese können nur durch ein Krebsregister gewonnen werden, das Grundlage für eine zukunftsorientierte Epidemiologie durch eine möglichst vollständige Datensammlung bietet.
Als erste Sicherungsmaßnahmen hat der Bundesminister für Gesundheit mit den sechs östlichen Bundesländern am 31. Dezember 1991 ein Verwaltungsabkommen geschlossen. Demgemäß hat das Bundesgesundheitsamt das Krebsregister für das Jahr 1992 in Verwahrung genommen. Es hatte auch die jetzt (auf freiwilliger Grundlage) erstatteten Meldungen entgegenzunehmen.
Für dieses Abkommen war vom Freistaat Sachsen als einem der beteiligten Länder eine Auflösungsklausel gefordert worden für den Fall, daß ein eigenes Krebsregister auf eigener rechtlicher Grundlage eingerichtet würde. Diese Bestimmung sollte sich auf die frühzeitigen Bestrebungen des Freistaates Sachsen beziehen, gegebenenfalls ein eigenes Krebsregister einzurichten, falls eine dauerhafte Sicherung des Krebsregisters auf andere Weise nicht möglich sein würde.
Da dem Sächsischen Gesundheitsministerium in der Anfangszeit juristisches Personal nicht in ausreichendem Maße zur Verfügung stand, habe ich schon im August 1991 bei dem Entwurf eines Sächsischen Krebsregistergesetzes Formulierungshilfe geleistet. Die wiederholt geänderten Entwürfe habe ich grundsätzlich aus folgenden Gründen unterstützt:

- In der ehemaligen DDR bestand die zu einem hohem Meldestand führende Meldepflicht, die auch von der Ärzteschaft akzeptiert wurde und heute noch wird. Der rational nicht zu begründenden Auffassung, eine Meldepflicht "stigmatisiere" Krebspatienten, weil diese Krebskranke solchen Patienten gleichstelle, die an einer ansteckenden Krankheit leiden (so Begründung des Entwurfs eines Bundeskrebsregistergesetzes, Stand 29.01.93, S. 24), kann ich kein Verständnis entgegenbringen.

- Es gilt, möglichst bald Anschluß zu erreichen an das Krebsregister der ehemaligen DDR, damit dieser wertvolle Datenbestand nicht durch lückenhafte Nachmeldungen entwertet wird.

- Eine gesetzlich vorgeschriebene Einwilligung des Patienten wird zwangsläufig zu einem unvollständigen Meldestand führen. Ein unter einer Melderate von 90 % liegender Bestand macht andererseits nach übereinstimmender Auffassung der Epidemiologen den wissenschaftlichen Wert von Krebsregistern zunichte. Den - an dem mangelnden Erfolg gemessenen - immensen Aufwand eines derartigen Krebsregisters kann man sich ersparen. Die Steuermittel ließen sich dann besser einsetzen.

- Eine Kopplung des ärztlichen Melderechts an die Einwilligung des Patienten setzt dessen volle Aufklärung über seinen Gesundheitszustand und den voraussichtlichen Krankheitszustand voraus. Ich lehne eine derartige Kopplung ab, weil es alleinige Entscheidung des Arztes bleiben muß, ob, wann und inwieweit er seine Patienten aufklärt. Das berufsethische Interesse des Arztes an einer Meldung an das Krebsregister darf kein Grund für eine Aufklärung des Patienten über Stadium und Verlauf seiner Erkrankung sein. Das Persönlichkeitsrecht erschöpft sich nicht im Datenschutz.

- Für sehr wichtig halte ich, daß der Registerstelle eine unabhängige Vertrauensstelle (unter ärztlicher Leitung sowie mit Personal, das als ärztliches Fachpersonal i. S. der Schweigepflicht und des Beschlagnahmeschutzes gilt) vorgeschaltet wird, welche die Identitätsdaten in verschlüsselter Form an die Registerstelle weiterleitet. Damit kann die Registerstelle die epidemiologischen Daten keiner Person mehr zuordnen.

Der Entwurf eines eigenständigen Sächsischen Krebsregistergesetzes wurde gegenstandslos, nachdem der Bund am 12. November 1992 ein Krebsregistersicherungsgesetz verabschiedet hat, das Ende 1994 außer Kraft treten wird. Dieses Gesetz sichert die Daten des "Nationalen Krebsregisters" der ehemaligen DDR, das als gemeinsames Register der sechs östlichen Bundesländer weitergeführt wird. Das Gesetz sieht ein *Recht* der Ärzte zur Meldung an das Register vor. Die Meldungen bedürfen der Einwilligung des Patienten. Das Verfahren kann allerdings durch Landesgesetz abweichend bestimmt werden.

Letzter Stand ist, daß das Sächsische Kabinett den Entwurf eines Durchführungsgesetzes zum Krebsregistersicherungsgesetz verabschiedet hat. Der Gesetzentwurf sieht eine ärztliche Melde*pflicht* vor, einer Einwilligung der Patienten in die Meldung bedarf es nicht. Die Ärzte unterrichten ihre Patienten über die Meldung, jedoch nur sofern dies verantwortbar ist. Ich trage diese Initiative des Gesundheitsministers aus den oben geschilderten Gründen mit, obwohl eine Vertrauensstelle aus technischen Gründen noch nicht zwischengeschaltet sein kann. Das nach Außerkrafttreten des Krebsregistergesetzes vorgesehene Bundeskrebsregistergesetz, durch das die Länder zur Einrichtung von Krebsregistern nach einheitlichen Maßstäben verpflichtet werden sollen, wird eine Vertrauensstelle unter ärztlicher Leitung vorsehen. Diese sollte nach meinen Vorstellungen als Selbstverwaltungseinrichtung der Ärzteschaft errichtet werden.

10.1.3 Register über Patienten mit Mukoviszidose (CF-Register)

An der Kinderklinik der Medizinischen Akademie Dresden (MAD) wurde vor der Wiedervereinigung für die DDR ein Register über Patienten geführt, die an Mukoviszidose erkrankt sind (CF-Register). Es handelt sich um eine Stoffwechselerkrankung, die unbehandelt früher schon im Kleinkindesalter zum Tod führte. Bei optimaler Betreuung beträgt heute die Lebenserwartung durchschnittlich 25 Jahre; im Einzelfall liegt sie auch weit darüber. Nach Auffassung der MAD spielt das Register bei der Optimierung der Behandlung eine wesentliche Rolle, weil dadurch die Möglichkeit einer Analyse der Krankheitsverläufe sowie des Einflusses neuer Behandlungsstrategien geschaffen werde.
Das Register wird in Dresden zur Zeit für die fünf neuen Länder einschließlich Berlin fortgeführt.
Ein ähnliches Register besteht an der Universitätsklinik in Frankfurt am Main für die alten Länder. Geplant ist eine Vereinigung; über den Sitz des Registers ist noch nicht entschieden worden.

Die Problematik weist eine Reihe von Parallelen mit der Fortführung des Krebsregisters der DDR auf. In diesem Falle wurde eigens ein Bundesgesetz, das Krebsregistersicherungsgesetz, verabschiedet und auf Landesebene ein Krebsregistergesetz entworfen. Langfristig werden ähnliche Schritte auch beim CF-Register erforderlich sein. Zunächst jedoch muß einerseits der Bestand und die Fortführung gesichert, andererseits eine Anpassung an datenschutzrechtliche Anforderungen erreicht werden. Aus diesem Grunde haben Gespräche zwischen der MAD und mir über die Gestaltung des Meldeverfahrens stattgefunden. Gemeinsam wurde eine detaillierte Einwilligungserklärung der Patienten ausgearbeitet.

10.1.4 Auflösung von Polikliniken

Träger von Polikliniken waren neben Betrieben auch Gemeinden, kreisfreie Städte und Landkreise. Bei der Auflösung dieser Polikliniken stehen die Kommunen und Landkreise häufig vor großen Problemen bei der Sicherung und Aufbewahrung der Patientenunterlagen.

Ein Bürger beklagte sich z. B. darüber, daß ein Landratsamt Patientenunterlagen - unter anderem auch seine - der vom Landkreis übernommenen Poliklinik an sich gebracht habe, ohne die Patienten zu informieren und um ihre Einwilligung zu bitten. Das Landratsamt weigere sich nun, ihm seine Patientenunterlagen auszuhändigen, die er für ärztliche Behandlung dringend benötige.

Eine Anfrage bei dem Landratsamt ergab, daß es die Unterlagen sicherstellen mußte, weil das einem Industriebetrieb gehörende Gebäude bei Auflösung der Klinik geräumt werden mußte. Aus organisatorischen Gründen, u. a. wegen der großen Zahl der Patienten, sei es nicht möglich gewesen, diese vorher um Einwilligung zu bitten. Zuge-

sagt wurde mir, in Zukunft nicht mehr - wie vorher Praxis - diese Unterlagen dem behandelnden Arzt auf dessen einfache Anforderung zuzusenden, sondern sie nur mit schriftlicher Einwilligung des Patienten einem Arzt auszuhändigen. Im Einzelfall könnte die Aushändigung der Krankenpapiere an den Patienten selbst aus ärztlichen Gründen nicht angeraten sein. Keinesfalls sollte die übliche Regelung, daß der Arzt zu entscheiden hat, ob, wann und wie weit der Patient informiert wird - die volle Unterrichtung ist heute die Regel - staatlich gelenkt oder beeinflußt werden.

Dem Bürger habe ich die Rechtslage erläutert. Die sichere Aufbewahrung durch ein Landratsamt, dessen Mitarbeiter zur Verschwiegenheit verpflichtet sind und die sich bei Verletzung dieser Verschwiegenheitspflicht strafbar machen, stellt unter den schwierigen Umständen, insbesondere der "Wendezeit", das datenschutzrechtlich kleinere Übel dar. Ich habe ihm geraten, seine Patientenunterlagen mit schriftlicher Einwilligung durch seinen Arzt anfordern zu lassen.

Das Sächsische Staatsministerium für Soziales, Gesundheit und Familie habe ich um eine Liste der aufgelösten Polikliniken und weitere Auskünfte, die Aufschluß über den Verbleib der Patientenunterlagen geben können, gebeten, bisher leider ohne Resonanz.

10.1.5 Kontroll- und Informationsbesuch in einer Fachklinik

Im März 1992 fand ein Kontroll- und Informationsbesuch in einer Fachklinik statt.

Die Organisation der gesamten Einrichtung befand sich im Neuaufbau. Das Führungspersonal war teilweise erst wenige Tage im Amt. Es konnten daher noch keine bereits vorhandenen Strukturen überprüft werden, aber es war möglich eine Fülle organisatorischer Fragen, insbesonderer im Zusammenhang mit den neuen datenschutzrechtlichen Bestimmungen, zu erörtern.

1. Archivwesen und Altdatenbestände befanden sich in einem gesondert gesicherten Gebäude, das schon zu Zeiten der DDR als Archivgebäude genutzt worden war. Hier wurden abgeschlossene Patientenakten in Regalen geordnet abgelegt. Stichproben ergaben, daß sie offensichtlich vollständig waren. Die Patientenunterlagen gehen bis zur Jahrhundertwende zurück. Zur Frage einer Aussonderung werde ich Stellung nehmen, sobald Klarheit über die Gesetzeslage besteht.

2. Personalwesen: Die Personalakten wurden zum Großteil noch nach dem System der ehemaligen Kaderakten der DDR geführt. Sie sollten nach Auskunft der Klinikleitung vollständig überarbeitet werden. Am Beispiel des neuen Personalbogens, dessen Einführung beabsichtigt war, wurden die zulässigen und unzulässigen Fragen zur Person eines Bediensteten (z. B. die Angabe und weitere Verwendung der PKZ) mit der Klinikleitung und den zuständigen Mitarbeitern im einzelnen besprochen.

Der PC in der Personalabteilung war noch nicht einsatzbereit. Die Verantwortlichen wurden darauf hingewiesen, daß durch technische und organisatorische Maßnahmen die Einhaltung von § 9 SächsDSG sicherzustellen ist. Dem Systemverwalter war bekannt, daß hierbei besondere Maßnahmen beim Einsatz von Personalcomputern mit dem Betriebssystem MS-DOS erforderlich sind.

3. Die Datenverarbeitungstechnik befand sich, wie erwähnt, noch im Aufbau. Vorgesehen waren ein zentrales UNIX-Netzwerk mit 10 Terminals und 2 PCs, ein PC in der Personalverwaltung und 10 PCs für die Textverarbeitung der Stationen. Ich habe in diesem Zusammenhang insbesondere darauf hingewiesen, daß künftige Nutzer nur Zugriff zu den Daten haben dürfen, die zur Erfüllung *ihrer* Aufgaben erforderlich sind. Entsprechend müssen Vordrucke, Aufkleber etc. gestaltet sein. Der Pförtner z. B. benötigt zur Auskunftserteilung keine Diagnosedaten.

Im Rahmen einer Stichprobe habe ich einen PC in einer Fachabteilung überprüft. Auf der Festplatte waren nur wenige Textdateien gespeichert. Es handelte sich überwiegend um ärztliche Berichte und Therapieprotokolle mit äußerst schutzwürdigen Angaben zur Person (Anamnese- und Diagnosedaten) des jeweiligen Patienten, die dem Arztgeheimnis unterliegen. An Hand dieser Textdateien konnte ich den Anwesenden demonstrieren, welche Daten Unbefugten auch ohne besondere Datenverarbeitungskenntnisse zur Verfügung stehen, wenn - wie hier - die Sicherung dieser Daten nicht gewährleistet ist.

Vom Leiter der Fachklinik wurde zugesagt, die Mängel, von denen er bis dahin keine Kenntnis hatte, sofort zu beseitigen und die dazu erforderlichen organisatorischen und technischen Maßnahmen zu ergreifen.

Nach Durchführung der Umstellung werde ich die Fachklinik erneut kontrollieren.

10.1.6 Zusammenarbeit zwischen Regierungspräsidien und der Landesapothekerkammer

Die Regierungspräsidien sind zuständig für sogenannte apothekenrechtliche Entscheidungen. Dabei handelt es sich insbesondere um die Erlaubnis zum Betrieb (§ 2 Gesetz über das Apothekenwesen) und zur Verpachtung einer Apotheke (§ 9 Gesetz über das Apothekenwesen). In bestimmten Fällen, etwa wenn ein Bewerber aus einem anderen Bundesland diese Erlaubnis beantragt, sind die Regierungspräsidien auf einen Informationsaustausch mit der Landesapothekerkammer angewiesen, der auf eine einwandfreie rechtliche, also gesetzliche Grundlage gestellt werden muß. Mit dem Sächsischen Staatsministerium für Soziales, Gesundheit und Familie (SMS) und der Landesapothekerkammer habe ich Einigkeit erzielt, daß eine Verwaltungsvorschrift nicht ausreicht. Daher wird das SMS im Zusammenwirken mit der Landesapothekerkammer und mir eine gesetzliche Regelung erarbeiten.

10.1.7 Übermittlung von Patientendaten von Ausländern an das Konsulat des Heimatstaates

Ausländer können bei einem Unfall in Sachsen verletzt werden oder erkranken. Sollen die Angehörigen des Betroffenen in der Heimat benachrichtigt werden, so ist das auf verschiedenen Wegen möglich, auch über die Einschaltung eines Konsuls ihres Heimatlandes.
Dem Generalkonsul eines ehemaligen "Ostblockstaates" werden von den Ärzten in sächsischen Krankenhäusern Informationen über die betroffenen ausländischen Bürger zuweilen gegeben, aber auch verweigert. Die Verweigerung von Auskünften wurde von Ärzten z. B. damit begründet, daß solche Informationen nur an Familienangehörige weitergegeben werden dürfen. Der Generalkonsul möchte nun von dem zuständigen Staatsministerium eine *generelle* Regelung, daß Krankenhäuser Informationen über den Zustand kranker oder verletzter Ausländer an das Konsulat grundsätzlich nicht verweigern sollen. Diese Information möchte der Konsul z.B. unmittelbar an die Familienangehörigen in der Heimat weiterleiten. Das Staatsministerium wandte sich an den Sächsischen Datenschutzbeauftragten um Stellungnahme.

Bei Angaben über den Gesundheitszustand von Menschen handelt es sich um personenbezogene Daten, die besonders schutzwürdig sind. Sofern der verletzte oder erkrankte Ausländer nicht von sich aus freiwillig und ausdrücklich zustimmt, daß das jeweilige Konsulat über seinen Gesundheitszustand unterrichtet wird, ist die gewünschte Information an das Konsulat nicht statthaft; sie verletzt das Grundrecht auf informationelle Selbstbestimmung.

Den behandelnden Ärzten und dem mit ihnen zusammenarbeitenden Personal ist es im allgemeinen untersagt, Angaben zum Zustand der ihnen anvertrauten Patienten zu machen. Nach § 203 des Strafgesetzbuches kann jedenfalls nicht generell von "mutmaßlicher Einwilligung" des Betroffenen in eine solche Datenübermittlung ausgegangen werden.

Denkbar sind auch Sonderfälle. Führen diese zu einer anderen Beurteilung? Bei allem Verständnis für menschliche und Sprachprobleme, die beim Unfall eines Ausländers in Sachsen auftreten können, kann auch in außergewöhnlichen Situationen (z. B. Bewußtlosigkeit nach Unfall) nicht von einer mutmaßlichen Einwilligung in die Erteilung detaillierter Auskünfte über den Zustand des Betroffenen an das jeweilige Konsulat ausgegangen werden. Es kann auch nicht angenommen werden, daß über den Konsul die Angehörigen stets wesentlich schneller unterrichtet werden können, als wenn dies unmittelbar oder über Hilfsorganisationen (kirchliche Dienste, Internationales Rotes Kreuz) geschieht.

Anders ist die Situation bezüglich Angehöriger: Hier kann eine mutmaßliche Einwilligung in die Unterrichtung vom Zustand des Verletzten vorausgesetzt werden. Einer unmittelbaren Kontaktaufnahme zwischen Arzt bzw. Krankenhaus und Angehörigen

im Heimatland steht bei Bewußtlosigkeit oder Tod also nichts entgegen. Die Verbindung kann dabei auf verschiedenen Wegen hergestellt werden, z. B. auch über das Rote Kreuz oder über die Kirche; die Einschaltung staatlicher Stellen, die manchmal auch aus anderen Gründen interessiert sind, sollte vermieden werden, zumal dann, wenn der betreffende Staat das Persönlichkeitsrecht (noch) nicht in ähnlicher Weise schützt, wie dies in Deutschland geschieht.
Ärzte und Krankenhauspersonal, die dem Konsulat keine Auskunft über den Gesundheitszustand des ausländischen Patienten geben, handeln damit verantwortungsvoll und gemäß geltendem Recht.
Selbstverständlich steht es dem Betroffenen frei, sich selbst zu entscheiden, ob er sich an seine eigenen Angehörigen wendet, kirchliche oder karitative Einrichtungen seines Vertrauens wählt oder sich an sein zuständiges Konsulat wendet, um seine persönlichen Interessen wahrnehmen zu lassen. Welche Information er dabei jedoch weitergibt, kann er auf Grund seines Rechts auf informationelle Selbstbestimmung nach freiem Ermessen selbst festlegen.
Die von dem erwähnten Generalkonsul vom Staatsministerium gewünschte generelle Regelung verletzte das Recht auf informationelle Selbstbestimmung und andere Rechtsvorschriften, sie wäre demnach so nicht statthaft.

10.1.8 Projekt "Ambulante onkologische Versorgung"

Im Zuge dieses Vorhabens des Sächsischen Staatsministeriums für Soziales, Gesundheit und Familie wurde zunächst eine Bestandsaufnahme der onkologischen Versorgung in der ehemaligen DDR durchgeführt. Auf dieser Grundlage soll ein therapeutisches Konzept entwickelt werden, über das eine Vereinbarung zwischen den Sächsischen Krankenkassenverbänden und der Kassenärztlichen Vereinigung Sachsen getroffen werden soll.
Im Rahmen der Bestandsaufnahme wurden Patienten der ehemaligen Beratungsstellen befragt. Der dazu verwendete Fragebogen ist anonym; gegen seinen Inhalt bestehen keine Einwände. Meiner Anregung, daß die Befragung durch fähige Interviewer und nur nach Einwilligung des behandelnden Arztes stattfinden soll, wurde vom Ministerium entsprochen.

10.1.9 Impfdokumentation

Das Sächsische Staatsministerium für Soziales, Gesundheit und Familie (SMS) hat einen Organisationserlaß zur Dokumentation von Schutzimpfungen entworfen. Es war vorgesehen, daß impfende Ärzte, häufig niedergelassene Ärzte, alle Impfungen in der Reihenfolge ihrer Durchführung für jeden Kalendermonat listenmäßig erfassen und diese Listen in jedem Quartal an das zuständige Gesundheitsamt weiterleiten. An Hand der Impflisten sollten die Gesundheitsämter Impfkarteien erstellen, in denen die Impflinge namentlich aufgeführt sind. Beabsichtigt war weiterhin auf der Grundlage der Impflisten und der Geburtenmeldungen eine halbjährliche Meldung des Gesundheitsamts an das örtlich zuständige Institut der Landesuntersuchungsanstalt für das Gesundheits- und Veterinärwesen über die durchgeführten Impfungen. Diese

Meldungen sollten für die einzelnen Geburtsjahrgänge erfolgen, also nicht personenbezogen.

Ziel war es, einen Überblick über die Impfsituation in Sachsen zu erhalten, und in dem Falle, daß Impfdokumente verlorengehen, eine Doppelimpfung zu vermeiden.

Ich habe mit dem SMS Einigkeit darüber erzielt, daß ein Erlaß keine geeignete Regelungsform ist. Insbesondere für eine Meldepflicht gegenüber dem Gesundheitsamt, die für die Ärzte gelten soll, welche die empfohlene Impfung durchführen, bedarf es nach meiner Auffassung einer gesetzlichen Grundlage, die bei den *empfohlenen* Impfungen fehlt. Bei Pflichtimpfungen genügt möglicherweise § 14 Bundesseuchengesetz; diese Impfungen spielen z. Zt. in der Praxis keine Rolle.
Der impfende Arzt unterliegt der ärztlichen Schweigepflicht, die durch § 203 Abs. 1 Strafgesetzbuch (StGB) geschützt wird. Eine Befugnis zur Geheimnisoffenbarung aufgrund einer gesetzlichen Regelung besteht bei empfohlenen Schutzimpfungen nicht. Erforderlich ist daher die Einwilligung des Impflings bzw. seiner gesetzlichen Vertreter.

Das SMS wird das Verfahren nicht in einem Erlaß regeln, sondern Empfehlungen auf der Grundlage meiner Stellungnahme und in Abstimmung mit mir erarbeiten.

10.2 Sozialwesen

10.2.1Angaben bei Erstantrag auf Sozialhilfe

Mit einem Regierungspräsidium ist es zu einer Diskussion über die Frage gekommen, welche Angaben bei einem Erstantrag auf Sozialhilfe verlangt werden dürfen. Ich habe z. B. kritisiert, daß ein Formular sich nicht auf die Frage nach Schenkungen des Antragstellers in den letzten 10 Jahren beschränkte, sondern darüber hinaus auch die Person des Beschenkten angegeben werden sollte.
Grundsätzlich ist die Frage nach Schenkungen berechtigt. Gemäß § 528 Abs. 1 Bürgerliches Gesetzbuch (BGB) hat derjenige, der auf Grund einer Schenkung nicht mehr in der Lage ist, seinen angemessenen Unterhalt zu bestreiten oder seine Unterhaltspflichten zu erfüllen, einen Herausgabeanspruch gegen den Beschenkten. Gemäß § 529 Abs. 1 BGB ist dieser Anspruch ausgeschlossen, wenn zur Zeit des Eintritts der Bedürftigkeit 10 Jahre seit der Schenkung verstrichen sind. Diesen Anspruch kann der Träger der Sozialhilfe gemäß § 90 Abs. 1 Bundessozialhilfegesetz (BSHG) auf sich überleiten. Grundsätzlich ist die Behörde daher berechtigt, nach Schenkungen zu fragen. Wünschenswert ist es jedoch, im Antragsformular Kriterien für den Wert der Schenkung zu nennen, um so eine unnötige Erhebung von Daten über Bagatellschenkungen, die sich nicht auf den Sozialhilfeanspruch auswirken, zu vermeiden.

Ein Problem liegt auch darin, ob ein Zeitraum von 10 Jahren erfaßt werden darf oder ob auf den Zeitpunkt des Inkrafttretens des Bundessozialhilfegesetzes in den neuen Bundesländern am 1.1.1991 abgestellt werden muß.
Nicht erforderlich ist vor allem die Frage nach der Person des Beschenkten. Zum Zeitpunkt der Antragstellung ist nicht absehbar, ob Sozialhilfe überhaupt gewährt oder der Antrag aus von der Schenkung völlig unabhängigen Gründen abgelehnt wird. Wichtig wird die Kenntnis der Person des Beschenkten erst dann, wenn die weiteren Voraussetzungen eines Rückforderungsanspruchs zu prüfen sind und die Überleitung gemäß § 90 BSHG erfolgen soll. Zum Zeitpunkt der Antragstellung genügt es also, wenn das Sozialamt weiß, ob eine Schenkung vorgenommen wurde oder nicht. Erst für das weitere Verfahren ist unter Umständen die Person des Beschenkten zu erfragen.

Ich habe die Anregung des Regierungspräsidiums begrüßt, unter Einbeziehung der Landratsämter in einem gemeinsamen Gespräch die Antragsformulare in diesem und in weiteren Punkten auf ihre Übereinstimmung mit den Anforderungen des Datenschutzes zu überprüfen. Eine erste Gesprächsrunde hat bereits stattgefunden. Sie wird demnächst fortgesetzt.

10.2.2 Antragsformulare für Kinder- und Jugendhilfe

Das leidige Problem der Antragsformulare trat auch im Bereich der Kinder- und Jugendhilfe auf. Als Beispiel sei ein langwieriger Schriftwechsel mit einem Landratsamt geschildert:
Gemäß § 13 Abs. 2 Satz 3 des Gesetzes zur Förderung von Kindern in Tageseinrichtungen im Freistaat Sachsen hat der örtliche Träger der öffentlichen Jugendhilfe auf Antrag den Elternbeitrag zu übernehmen, soweit die Belastung den Eltern gemäß § 90 Abs. 3 und 4 Kinder- und Jugendhilfegesetz (KJHG) nicht zuzumuten ist. Bezüglich der Feststellung der Zumutbarkeit verweist § 90 Abs. 4 KJHG auf die § 76 bis 79, 84 und 85 Bundessozialhilfe-gesetz (BSHG).
Zunächst war zu bemängeln, daß im Zuständigkeitsbereich des Landratsamts die für Anträge auf *Übernahme* der Elternbeiträge ausgearbeiteten Vordrucke stattdessen für die Vorbereitung der *Festsetzung* der Elternbeiträge verwendet wurden, also an diejenigen Eltern ausgegeben wurden, die *selbst* die Beiträge entrichten müssen. Das Landratsamt hat zugesagt, diese Praxis unverzüglich zu ändern.
Aber auch der Inhalt des Vordrucks gab Anlaß zur Kritik. Gemäß § 62 Abs. 1 KJHG dürfen personenbezogene Daten nur erhoben werden, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. Diese Erforderlichkeit ist bei der Frage nach dem Geburtsdatum der Eltern zu verneinen. Die Angabe ist nicht erforderlich, um, wie vom Landratsamt zunächst eingewandt, eine Verwechslungsgefahr bei Namensgleichheit auszuschließen, da es nicht anzunehmen ist, daß sowohl der Vater als auch die Mutter des Kindes denselben Vor- und Zunamen tragen wie ein anderes Elternpaar. Falls eine Namensgleichheit - etwa bei einem alleinerziehenden Elternteil – auftreten sollte, steht zur Identifizierung noch die Adresse zur Verfügung. Eine Verwechslungsgefahr besteht also nicht. Das hat das

Landratsamt eingesehen.

Gefragt wurde nach dem "Einkommen mtl. Netto (Verdienstbescheinigung beifügen)" und "weiteren Einkünften (mtl.), z. B. aus Rente, Arbeitslosengeld, Kindergeld".
Zum Einkommen gehören alle Einkünfte in Geld oder Geldeswert mit Ausnahme bestimmter Einkünfte (§ 76 Abs. 1 BSHG). Abzusetzen von den Einkünften sind jedoch Steuern, Pflichtbeiträge zur Sozialversicherung, Beiträge zu anderen Versicherungen und die mit der Erzielung des Einkommens verbundenen notwendigen Auslagen (§ 76 Abs. 2 BSHG). Der verwendete Vordruck erfaßt jedoch nicht alle zu berücksichtigenden Abzüge. Z. B. nicht die mit der Erzielung des Einkommens verbundenen Auslagen, die in der "Verordnung zur Durchführung des § 76 des Bundessozialhilfegesetzes" vom 28. November 1962 (Bundesgesetzblatt Teil I, S. 692; geändert durch Verordnung vom 23.11.1976, Bundesgesetzblatt Teil I, S. 3234) näher definiert werden. Dazu gehören z. B. notwendige Aufwendungen für Fahrten zwischen Wohnung und Arbeitsstätte, weiterhin Mehraufwendungen bei doppelter Haushaltsführung. Das Formular muß also Platz vorsehen, in dem der Antragsteller solche Aufwendungen eintragen kann.

Nicht einsichtig ist auch die Frage nach den weiteren Kindern im Haushalt der Eltern, die in einer späteren Fassung des Vordrucks geändert wurde in die Frage nach weiteren Personen im Haushalt der Eltern. Gemäß § 79 Abs. 2 Satz 1 Nr. 3 BSHG wird ein Familienzuschlag berechnet für "jede Person, die von den Eltern überwiegend unterhalten worden ist oder der sie nach der Entscheidung über die Sozialhilfe unterhaltspflichtig werden." Es kommt also nicht darauf an, ob diese Person im Haushalt der Eltern lebt, und ebensowenig darauf, wie alt sie ist (im Vordruck wird auch nach dem Geburtsdatum dieser Personen gefragt), sondern nur darauf, ob eine Unterhaltspflicht besteht. Die Fragestellung im Vordruck ist daher einerseits zu eng, weil sie nicht im Haushalt lebende, aber unterhaltsberechtigte Personen (z. B. die Mutter eines Elternteils) nicht erfaßt, andererseits zu weit, weil sie das Geburtsdatum erfragt, ohne daß diese Datenerhebung erforderlich ist.

Das Landratsamt hat zugesagt, diesbezügliche Änderungen auszuarbeiten und die gesamte Problematik in der zuständigen Arbeitsgruppe des Sächsischen Landkreistages anzusprechen.
Die kritische Überprüfung von Vordrucken konzentriert die Verfahrensbeteiligten auf die richtigen Fragen und dient dadurch der einwandfreien Sachbearbeitung.

10.2.3 Sicherung von Personalunterlagen für die Rentenberechnung

Große Probleme wirft in den neuen Bundesländern die Berechnung der Renten auf. Die Rentenversicherungsträger haben keine eigenen Unterlagen über Beiträge, die in der DDR gezahlt worden sind. Zur Verfügung stehen nur die *Ausweise für Arbeit und Sozialversicherung (SV-Ausweis)* und die Lohnunterlagen in den Betrieben.

Die Eintragungen im SV-Ausweis sind häufig keine geeignete Grundlage für die Rentenberechnung. Nach § 256 a Abs. 3 Sozialgesetzbuch Sechstes Buch (SGB VI) werden zur Ermittlung der Beitragsbemessungsgrundlage Arbeitsverdienst und Einkünfte, die vor dem 1. März 1971 den monatlich versicherten Betrag von 600,- DM übersteigen, berücksichtigt, wenn diese höheren Arbeitsverdienste und Einkünfte nachgewiesen werden. Ein vor diesem Zeitpunkt erzieltes höheres Einkommen als 600,- DM monatlich führt also zu einer höheren Rente. Dieser Nachweis kann jedoch nicht mit dem SV-Ausweis geführt werden, weil bis einschließlich 28.2.1971 nur ein monatliches Einkommen von bis zu 600,- DM bescheinigt worden ist. Zwar können gemäß § 256 a Abs. 3 SGB VI die höheren Einkommen glaubhaft gemacht werden; die überschreitenden Beiträge werden jedoch nur zu fünf Sechsteln berücksichtigt. Der Nachweis der tatsächlich geleisteten Beiträge kann also nur durch Bescheinigung des Arbeitgebers geführt werden. Dasselbe gilt, wenn die SV-Ausweise verlorengegangen sind oder vernichtet wurden, weil nach DDR-Recht eine Witwen- bzw. Witwerrente nicht gezahlt wurde und daher bei vielen kein Interesse an einer Aufbewahrung bestand. Diese Personen sind also darauf angewiesen, daß die Lohnunterlagen der Betriebe verfügbar sind.
Arbeitgeberbescheinigungen sind gemäß § 8 Anspruch- und Anwartschaftsüberführungsgesetz auch erforderlich für Personen, die einem Zusatzversorgungssystem angehört haben.
Vor diesem Hintergrund plant eine Stadt, die Lohn- und Gehaltsunterlagen ihrer (ehemaligen) Mitarbeiter für den Zeitraum von 1949 bis 1991 automatisiert aufzubereiten und die Daten entweder im automatisierten Abrufverfahren den Rentenversicherungsträgern zuzuleiten oder im Rahmen einer Kontenklärung bzw. eines Rentenantrags durch das Versicherungsamt der Stadt mit Zustimmung des Versicherten zu nutzen. Ich habe das vorbildliche Bemühen dieser Stadt, die Interessen ihrer Mitarbeiter zu wahren und zugleich die Belange des Datenschutzes zu beachten, begrüßt und Hinweise zur Ausarbeitung eines Sicherheitskonzepts gegeben. Anzumerken war jedoch, daß eine elektronische Speicherung personenbezogener Daten nicht immer zu Vorteilen, sondern u. U. auch zu Nachteilen bzw. Gefahren führen kann. Bei ständig genutzten Daten, also der noch bei der Stadt beschäftigten Mitarbeiter, überwiegen die Vorteile auf Grund der Möglichkeit eines ständigen Zugriffs auf diese Daten. Bei selten benutzten Daten, wie im Falle der bereits ausgeschiedenen Mitarbeiter, können jedoch die Nachteile überwiegen. Eine elektronische Speicherung solcher "Altdaten" führt möglicherweise zu unvertretbaren Kosten. Ein möglicher Zerfall der Akten ist kein zwingendes Gegenargument, da die in ihnen enthaltenen notwendigen Daten auf Belegbögen oder ähnlichem gesichert werden können.
Klärungsbedürftig ist auch die Einrichtung eines automatisierten Abrufverfahrens mit dem Rentenversicherungsträger. § 148 Abs. 3 SGB VI trifft Regelungen für einen automatisierten Abruf aus Dateien der Rentenversicherungsträger. Bei einem Abruf

aus von der Stadt geführten Dateien ist § 8 Abs. 1 Sächsisches Datenschutzgesetz (SächsDSG) zu beachten. Danach darf ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, nur eingerichtet werden, soweit ein Gesetz dies ausdrücklich zuläßt. Auch ist die Notwendigkeit eines solchen Verfahrens nicht erkennbar, weil der Rentenversicherungsträger die erforderlichen Daten (z. B. durch die "Bescheinigung über Arbeitsentgelte oder Arbeitseinkommen gemäß § 8 Abs. 1 Satz 2 AAÜG") abfragt.

Das Problem der Sicherung der Unterlagen für die Rentenberechnung stellt sich insbesondere auch bei der Liquidation von Betrieben bzw. bei ihrem Verkauf durch die Treuhandanstalt.

10.2.4 Auftragsdatenverarbeitung im Wohngeldverfahren

Zuständige Stellen für die Gewährung von Wohngeld und die erforderlichen Feststellungen für die Wohngeldberechnung sind die Wohngeldstellen der Kreisfreien Städte und Landkreise sowie der Gemeinden mit über 20 000 Einwohnern. Für die Berechnung, Zahlungsanordnung und kassentechnische Abwicklung existiert ein landeseinheitliches EDV-Verfahren. Dieses wird von drei mittlerweile privaten Rechenzentren (ehemalige DVZ) durchgeführt. Bisher wurden die in den Wohngeldstellen erhobenen und auf Erfassungsbelegen oder Disketten gespeicherten Daten von den Wohngeldstellen zu diesen Rechenzentren transportiert. Zur Zeit wird eine Datenleitung zwischen Wohngeldstellen und Rechenzentren eingerichtet.

Es handelt sich bei diesem Verfahren um eine Verarbeitung von Sozialdaten im Auftrag gemäß § 80 Sozialgesetzbuch Zehntes Buch (SGB X), an die besondere Anforderungen gestellt werden. Problematisch ist hier insbesondere, daß gemäß § 80 Abs. 5 SGB X eine Verarbeitung durch nicht-öffentliche Stellen nur zulässig ist, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge hierdurch erheblich kostengünstiger erledigt werden können.

Es mußten unter hohem Zeitdruck und auf der Grundlage sich wiederholt ändernder Regelungen durch das Wohngeldgesetz und das Wohngeldsondergesetz Wege gefunden werden, eine pünktliche Auszahlung an die Berechtigten zu gewährleisten. Zwischen dem für das Wohngeld zuständigen Staatsministerium des Innern, den beteiligten Unternehmen und mir sind die zahlreichen Probleme, zu denen auch die Frage der Ausgestaltung der Verträge zwischen dem Freistaat Sachsen und den Rechenzentren gehört, erörtert worden. Befriedigende Ergebnisse konnten bisher jedoch noch nicht in allen Fragen erzielt werden. Weitere Gespräche sind daher erforderlich.
Unerläßlich sind in Zukunft ordnungsgemäße Ausschreibungen der (privaten) Leistungen bei der Wohngeldberechnung im Auftrag, denn nur so kann die Frage, wer kostengünstiger als öffentlich-rechtlich getragene Rechenzentren arbeitet, nachvollziehbar beantwortet werden. Vermutungen reichen hier keinesfalls aus.
Jeder Verdacht einer Bevorzugung ehemals staatstragender Betriebe ist zu vermeiden.

10.3 Veterinärwesen: "Verbraucherschutz- und Gesundheits-Informations-System" (VEGIS)

VEGIS ist ein Informationssystem im Zuständigkeitsbereich des Sächsischen Staatsministeriums für Soziales, Gesundheit und Familie (SMS) zur Lebensmittelüberwachung, in der Humanmedizin (Arzneimittel) und in der Veterinärmedizin. Die eine Säule dieses Systems ist VEGIS (B) für innerstaatliche Behörden und die Europäischen Gemeinschaften, die andere VEGIS (L), das Informationssystem der Landesuntersuchungsanstalt.

Zuständig für Lebensmittelüberwachung und Veterinärmedizin sind die Lebensmittelüberwachungs- und Veterinärämter in den Landkreisen und kreisfreien Städten. Zu ihren Aufgaben gehört es insbesondere, Proben zu entnehmen, die der Landesuntersuchungsanstalt übergeben und von ihr ausgewertet werden. Auch werden von den Lebensmittelüberwachungs- und Veterinärämtern Rechtsverstöße, etwa gegen das Lebensmittel- und Bedarfsgegenständegesetz, geahndet.

Die von ihnen erhobenen personenbezogenen Daten bleiben (abgesehen von wenigen Ausnahmen) in ihrem Bereich. Im Zuge der regelmäßigen Unterrichtung werden an die Regierungspräsidien, das SMS und die Europäischen Gemeinschaften nur anonymisierte Daten übermittelt.

Ich wurde bereits frühzeitig in die Erarbeitung der Anforderungen an die Software des Informationssystems einbezogen. Meine Stellungnahmen waren daher dem Entwicklungsteam bekannt und konnten von ihm berücksichtigt werden.

11 Landwirtschaft, Ernährung und Forsten

11.1 Gläserner Landwirt

Es ist nicht unbekannt, daß ein oft reicher Goldsegen den EG-Mitgliedsstaaten zuteil wird, dessen Zweck, nämlich die Verwendung für landwirtschaftliche Maßnahmen, allzu oft verfehlt wird. Weniger bekannt ist die Gegenreaktion der EG-Bürokratie auf diese Tatsache: Die Einführung eines integrierten Verwaltungs- und Kontrollsystem durch die Verordnung (EWG) Nr. 3508/92 vom 27. November 1992. Ziel der Verordnung ist es, die verwaltungstechnischen Probleme, die bei flächenbezogenen Beihilfen entstehen, durch eine lückenlose Erfassung der Flächen (mit Nutzungsart) zu lösen. Die Landwirte haben die Flächen mit der Größe und der geographischen Lage anzugeben. Die Angaben sollen dann mit Satelliten- und Luftbildaufnahmen abgeglichen werden. Die Kontrollen sind umfassend und ohne das Vorliegen eines besonderen Anlasses vorgesehen: es entsteht der Gläserne Landwirt.

Das System ist zu neu und zu komplex, um es hinsichtlich seiner Auswirkungen auf

datenschutzrechtliche Fragen auch nur annähernd beurteilen zu können. Ich werde die Entwicklung auf diesem Gebiet jedoch besonders genau beobachten.

11.2 Öko-Landwirte

Die Arbeitsgemeinschaft Ökologischer Landbau hat bei mir angefragt, welche datenschutzrechtlichen Anforderungen an die Arbeit der privaten Kontrollstellen gestellt werden, welche die ökologischen Landbau treibenden Landwirte überwachen. Die Kontrollstellen würden in nicht unerheblichem Umfang auch in persönliche Angelegenheiten der Betriebsleiter Einblick nehmen und Dokumentationen erstellen.

Hierzu ist zu bemerken, daß nach der Verordnung (EWG) Nr. 2092/91 vom 24. Juni 1991 über den ökologischen Landbau, die unmittelbar geltendes Recht ist, jedes Unternehmen, das ökologische Erzeugnisse produziert, verpflichtet wird, sich einem routinemäßigen Kontrollverfahren zu unterziehen. Damit soll verhindert werden, daß Agrarprodukte unter der falschen Etikettierung als "Öko-Erzeugnisse" auf den Markt gebracht werden. Die Mitgliedstaaten können für das Kontrollverfahren Kontrollbehörden oder zugelassene private Kontrollstellen, die ihrerseits von einer Kontrollbehörde überwacht werden, einführen. In der Bundesrepublik Deutschland wurde der letztere Weg gewählt.

Meine Anfrage beim Sächsischen Staatsministerium für Landwirtschaft, Ernährung und Forsten, wie im Freistaat Sachsen vorgegangen werde, wurde dahin beantwortet, zuständige Kontrollbehörde sei die Sächsische Landesanstalt für Landwirtschaft, die zwei private Kontrollstellen anerkannt habe. Dreizehn weitere Kontrollstellen, die in anderen Bundesländern zugelassen sind, seien ergänzend zugelassen worden. Bislang liege lediglich der Entwurf einer vorläufigen Verwaltungsvorschrift zum Kontrollverfahren im ökologischen Landbau vor. Ich hatte bisher noch keine Gelegenheit, diesen Entwurf, nach dem offenbar bisher verfahren wurde, einzusehen. Eine Beurteilung, ob auf die Beachtung der datenschutzrechtlichen Vorschriften ausreichend hingewiesen wurde, ist mir daher nicht möglich.
Ich habe das Staatsministerium darauf aufmerksam gemacht, daß die privaten Kontrollstellen öffentliche Stellen im Sinne des § 2 Abs.2 Satz 1 SächsDSG sind, weil sie Aufgaben der öffentlichen Verwaltung wahrnehmen. Im übrigen werde ich darauf drängen, daß eine Verwaltungsvorschrift nach meiner Anhörung erlassen und veröffentlicht wird.

11.3 Forstorganisation

Der Regierungsentwurf des Sächsischen Waldgesetzes defininierte in § 37 die Aufgaben und Zuständigkeiten der Forstämter u.a. wie folgt:
- *Bewirtschaftung* und Verwaltung des Staatswaldes,
- Forsttechnische Betriebsleitung und forstlicher Revierdienst im Körperschaftswald,
- *Beratung,* Betreuung und technische Hilfe im Privatwald,
- Durchführung forstlicher Förderungsmaßnahmen,

- Ausübung der *Forstaufsicht* und des Forstschutzes.

Die Forstbehörde sollte demnach gleichzeitig - und verantwortlich geleitet durch ein und dieselbe Person, nämlich den Forstamtsleiter - sowohl Aufsichtsbehörde, Mitbewirtschafter und Beratungs- und Betreuungsorganisation sein. Dies, obwohl sie der größte Forstwirtschaftsbetrieb und damit marktbeherrschender Konkurrenzbetrieb der von ihr staatlich beaufsichtigten und betreuten kommunalen und privaten Forstbetriebe ist.

Eine derartige Aufgabenkombination ist in keinem anderen Bereich von Verwaltung und Wirtschaft bekannt und wohl kaum denkbar; sie ist allerdings z. B. in Baden-Württemberg so gewachsen.

Nach dem Volkszählungsurteil vom 15.12.1983 wird jedoch die Inkompatibilität dieser Aufgaben augenfällig, weil die notwendigen organisatorischen Vorkehrungen zur strikten Zweckbindung erhobener Daten im allzuständigen Forstamt fehlen: Das Wissen der staatlichen Aufsichts- und Betreuungsbehörde über private und kommunale Forstbetriebe darf nicht gleichzeitig zum Wissen von deren Marktkonkurrenten (Forstfiskus) werden. Die Organisationshoheit der Verwaltung wird auch durch den Schutz des Persönlichkeitsrechts beschränkt: Deshalb dürfen einer Behörde nicht gleichzeitig Aufgaben übertragen werden, die die Gefahr einer Zweckentfremdung von Daten mit sich bringen. Dieses Gebot der informationellen Gewaltenteilung mit der Konsequenz der Bildung funktional abgegrenzter (oder sogar abgeschotteter) Behörden wird vom Bundesverfassungsgericht postuliert. Gemäß § 9 Abs. 1 SächsDSG sind alle personellen, technischen und organisatorischen Maßnahmen zu treffen, um eine gesetzesgemäße, also auch zweckgebundene Datenverarbeitung in Dateien, Karteien oder Akten sicherzustellen.
Gegen die im Waldgesetzentwurf vorgesehene Aufgabenbündelung bei den (kleinen und intern nicht abgeschotteten) Forstämtern habe ich mich mit Nachdruck ausgesprochen, und ich habe meine Auffassung dem Landwirtschaftsausschuß in einem Kurzgutachten erläutert. Ich habe vorgeschlagen, die Aufsichtsfunktionen über die ca. 80 000 (z. T. sehr kleinen) sächsischen Forstbetriebe den Landratsämtern und die Beratungs- und Betreuungsaufgaben - solange Selbstverwaltungsorganisationen nicht vorhanden sind - den Landwirtschaftsämtern zu übertragen.
Dies stieß auf den entschiedenen, insbesondere mit Praktikabilitätsgründen vorgetragenen Widerstand des Landwirtschaftsministeriums.
Der Vermittlung des Ministerpräsidenten und zuletzt des Landtagspräsidenten ist es zu verdanken, daß das Landwirtschaftsministerium und ich den Fraktionen einen konsensfähigen Vorschlag unterbreiten konnten: Der Gesetzgeber hat demgemäß entschieden, daß die Forstaufsichts- und Forstschutzaufgaben (§ 40 Abs. 1 SächsWaldG) und die Durchführung forstlicher Förderungsmaßnahmen je einer organisatorischen Einheit der Forstdirektion übertragen werden, die keine anderen Aufgaben erfüllen (§ 37 Abs. 2 S. 2 SächsWaldG).

Damit ist eine datenschutzrechtlich gute Lösung gefunden worden; ich werde Gelegenheit nehmen, die Einzelheiten der Datenerhebung und -nutzung in den Forstdirektionen kennenzulernen und zu prüfen.
Der Zeitung habe ich am 3. März 1993 entnommen, daß das Landwirtschaftsministerium mitteile, jeder Waldeigentümer könne die Förderung der Wiederaufforstung bei den Forstämtern oder den Landwirtschaftsämtern beantragen. - Das entspricht nicht der gesetzlichen Zuständigkeit. Denn die verfassungskonforme Auslegung des Begriffs der "Durchführung forstlicher Förderungsmaßnahmen" schließt die Entgegennahme und Erstsichtung der Förderungsanträge und dazugehörenden Unterlagen ein. Diese Datenerhebung und "Erstverarbeitung" sollte ja gerade dem Forstamt versagt bleiben, weil es in erster Linie den Konkurrenzbetrieb "Staatsforstverwaltung" bewirtschaftet.
Die Antwort des Landwirtschaftsministeriums auf meine Frage, ob die gesetzlich vorgeschriebenen organisatorischen Vorkehrungen im Sinne einer Zweckbindung der Daten getroffen wurden, steht noch aus.

12 Umwelt und Landesentwicklung

EG-Umweltrichtlinie

Die EG-Richtlinie 90/313 gewährt jedermann ein voraussetzungsloses Recht auf Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt. Ziel dieser Richtlinie ist die Verbesserung des Umweltschutzes in der Gemeinschaft.

Der Bundesgesetzgeber hat die Richtlinie trotz einer bis zum 31.12.1992 von der EG gesetzten Frist noch nicht in nationales Recht umgesetzt. Nach der Rechtsprechung des Europäischen Gerichtshofs gelten damit seit dem 1.1.1993 die Vorschriften der Richtlinie als nationales Recht, soweit sie
a) vom Text her so bestimmt ausformuliert sind, daß sie - konkret - umsetzbar sind und
b) nicht in die Grundrechte, also z.B. in das informationelle Selbstbestimmungsrecht eines Betriebs- oder Grundstückeigentümers, eingreifen.
Das Staatsministerium für Umwelt, dem ich für seine vorbildliche Zusammenarbeit danke, hat mich frühzeitig bei der Erarbeitung einer Verwaltungsvorschrift eingeschaltet. Ich habe am 29.1.1993 folgende Auffassung vertreten:
"Nach nochmaliger eingehender Erörterung der Gesamtproblematik rege ich über Ihren Entwurf hinaus zu folgenden Überlegungen an:
Nach Art. 189 EWG-Vertrag ist eine Richtlinie (RL) im Gegensatz zur Verordnung grundsätzlich als zweistufiger Rechtsakt konzipiert (Bindung der Mitgliedstaaten zur Umsetzung in nationales Recht). Aus Gründen der Formenklarheit ist daher nur in begrenzten Ausnahmefällen eine unmittelbare Wirkung von RL möglich und in der Rechtsprechung des EuGH anerkannt (EuGHE 1982, S. 53 ff.). Es handelt sich dabei aber nur um solche Fälle, in denen die Vorschrift so "perfekt regelungsintensiv ausgestaltet ist, daß die Umsetzung der RL in nationales Recht sich mehr oder weniger in einem Abschreiben des RL-Inhalts erschöpfen müßte" (Oppermann, Europarecht, Beck München 1991 Rdnr. 466) und die verpflichteten Mitgliedstaaten die Anpassung ihres nationalen Rechts frist- und damit rechtswidrig nicht vorgenommen haben.

Diese herrschende Rechtsauffassung läßt mich daran zweifeln, ob - wie es die allgemeine Auffassung ist - die RL 90/313 am 1.1.1993 in allen Teilen direkt geltende Norm wurde. Denn eine normenklare Vorschrift insbesondere zu den gewichtigen Einschränkungen des Informationszugangs liegt unzweifelhaft nicht vor. Vielmehr fehlen - über einen Auslegungsbedarf, wie er bei jeder Norm aufkommen kann, hinaus - die wesentlichen Grundlagen dafür, ob und wieweit z. B. der nationale oder regionale Gesetzgeber in das Grundrecht auf informationelle Selbstbestimmung eingreifen oder weitere Restriktionen gemäß Art. 3 Abs. 2 und 3 der RL vorsehen kann.
Ich lasse dies jedoch offen, weil ich davon ausgehe, daß Sie diese Frage eingehend prüfen werden.

Ich trage die Absicht mit, eine Verwaltungsvorschrift im Freistaat Sachsen zu erlassen.

Ich bitte aber, daß die folgenden Kautelen eingehalten werden:

1. Wenn eine Verwaltungsvorschrift zur Auslegung der Richtlinie in Betracht kommt, ist es Aufgabe der Staatsregierung bzw. *aller* betroffenen Ressorts (SMI - Kommunen -, SMWK - Wissenschaft -, SML, SMWA, SMU), die selbst oder in ihrem nachgeordneten Bereich Aufgaben der Umweltpflege auf regionaler oder lokaler Ebene wahrnehmen, für eine *einheitliche* praktikable, umsetzungsfähige vorläufige Regelung zu sorgen.

   Deshalb ist eine Verwaltungsvorschrift des SMU allein keine anzustrebende Lösung. Ich halte eine weitergehende Abstimmung für unerläßlich, auch wenn dies zu einer kurzen zeitlichen Verzögerung führt. Ich halte mich dazu bereit, an gemeinsamen Verhandlungen unter der Federführung des SMU beratend teilzunehmen.

2. Art. 2 Buchst. a der RL enthält den Begriff der "*vorliegenden*" Information. Dieser Begriff verdeutlicht nicht nur, daß Behörden durch Informationsbegehren nicht zur Datenerhebung veranlaßt werden können, vielmehr ist er unter Bezug auf Art. 3 Abs. 3 dahin auszulegen, daß nur *gesicherte* Informationen die ausreichende Qualität einer sachlich richtigen Information über die Umwelt gewährleisten. Mutmaßungen, Behauptungen oder - wissenschaftlich ungesicherte - Rückschlüsse können dem Ziel einer Verbesserung des Umweltschutzes durch Informationszugang nicht dienlich sein. Deshalb sollen nur Daten "veröffentlicht" werden, die nach dem jeweiligen Kenntnisstand der Behörde den Tatsachen entsprechen.

3. Art. 2 Buchst. a betrifft u. a. Maßnahmen, die den Zustand der Umwelt "*beeinträchtigen*" oder "beeinträchtigen können". Es kommt nicht darauf an, ob solche Beeinträchtigungen rechtmäßig (z. B. weil bewilligt oder genehmigt) oder rechtswidrig vorgenommen werden. Allerdings wird der Kreis der Daten dadurch erheblich beschränkt; dabei ist zu bedenken, daß in Deutschland "die Umwelt" als *Kultur*land-schaft ausgeprägt ist.

4. Eine (untergesetzliche) Verwaltungsvorschrift darf keinesfalls in Grundrechte

eingreifen; der verfassungsrechtlich eindeutige Gesetzesvorbehalt verbietet dies. Die in Art. 3 Abs. 2 und 3 enthaltenen Regelungsspielräume dürfen daher jedenfalls in Bezug auf die - in der Bundesrepublik Deutschland grundgesetzlich garantierte - "Vertraulichkeit personen-bezogener Daten" (Abs. 2, 5. Tiret) durch eine Verwaltungsvorschrift *nicht zu Lasten des Datenschutzes* genutzt werden.

Die Richtlinie respektiert den Datenschutz ausdrücklich. Sie ist in ihren normenunscharfen Bereichen durch die Verwaltungsvorschrift *grundrechtskonform auszulegen*.

5. Sind die Behörden nur deshalb im Besitz von personenbezogenen (auch auf Personen beziehbaren) Daten, weil diese freiwillig übermittelt (Art. 3 Abs. 2, 6. Tiret) oder ohne gesetzliche Grundlage (also entgegen Art. 33 Sächsische Verfassung) erhoben wurden, muß von einer Veröffentlichung dieser Daten abgesehen werden, es sei denn, die Einwilligung des Betroffenen wird unter Beachtung des Verfahrens gemäß § 4 Abs. 2 und 3 Sächsisches Datenschutzgesetz eingeholt (siehe dazu 7 b).

6. Art. 3 Abs. 1 sieht einen Informationsanspruch ohne Nachweis eines Interesses vor. Dieser Anspruch vermag eher restriktiv (wie in Art. 3 Abs. 2 vorgesehen) ausgelegt werden als der sich aus Art. 34 der Sächsischen Verfassung ergebende Auskunftsanspruch, der sich auf diejenigen Daten beschränkt, die den Lebensraum des Individuums betreffen.

7. Aus den vorgenannten Gründen kommt - vorbehaltlich einer gesetzlichen Regelung - eine einschränkende, das informationelle Selbstbestimmungsrecht als Grundrecht weitgehend schützende, also eine verfassungskonforme Auslegung der Richtlinie in Betracht:
   a) Grundsätzlich sind amtlich festgestellte Daten (gesicherte Informationen mit ausreichender Qualität) in aggregierter oder anonymisierter Form bereitzustellen: Eine Anonymisierung liegt gemäß § 3 Abs. 1 Nr. 4 Sächsisches Datenschutzgesetz nur vor, wenn die Information nicht mehr einer bestimmten oder bestimmbaren Person zugeordnet werden kann.

   b) In allen anderen Fällen ist der Betroffene (wenn die Richtlinie in Art. 3 Abs. 2, 6. Tiret vom "Dritten" spricht, so meint sie u. a. auch den Betroffenen) vor der Preisgabe der ihn betreffenden Daten zu hören. Soweit dieser darlegt, daß er zur Meldung der Daten an die Behörde nicht gesetzlich verpflichtet wäre, *oder* er nachvollziehbar auf ein Privat- oder Geschäftsgeheimnis oder ein anderes geschütztes Interesse verweist, hat die Preisgabe der Information grundsätzlich zu unterbleiben. Wurden die Daten zweckgebunden und ohne gesetzliche Auskunftspflicht, z. B. in Förderungsverfahren, vom Betroffenen an die Behörde übermittelt, wirkt die grundrechtlich geschützte Zweckbindung dieser Daten durchgreifend. Dies ist beispielsweise bei allen Betriebsdaten ordnungsgemäß tätiger Land- und Forstwirte der Fall, es sei denn, diese Daten ergeben sich aus konkret genehmigungspflichtigen Vorgängen zu Maßnahmen, die

"beeinträchtigend" sind oder wirken können (dies schließt meist ihre Genehmigungsfähigkeit aus). Der Schutz solcher Betriebsdaten ist auch zur Aufrechterhaltung eines lauteren Wettbewerbs geboten.

Will die Behörde nach sorgfältigem Abwägungsprozeß trotz eines entgegenstehenden Willens des Betroffenen die Information erteilen, hat sie nach den Regeln über Verwaltungsakte mit Drittwirkung zu verfahren. Der Bescheid ist zunächst dem Betroffenen zuzustellen und darf gegenüber dem Auskunftsberechtigten erst vollzogen werden, wenn er bestandskräftig geworden ist.

c) Immer da, wo ein Personenbezug der Umweltinformation nicht hergestellt werden kann (z. B. bei parzellenunscharfen, größeres Terrain betreffenden Daten, bei Daten, die das Eigentum bzw. den Besitz nicht berühren (z. B. Grundwasser, höherer Luftraum) sowie in Bezug auf alle Daten, die auf gesetzlicher Grundlage (zwangsweise) ermittelt oder erhoben werden, um den Zustand der Umwelt festzustellen oder zu bewerten, bleibt das Informationsinteresse des Einzelnen vorrangig, es sei denn, die Vertraulichkeit der Beratung von Behörden, die internationalen Beziehungen, die Landesverteidigung, die öffentliche Sicherheit sind berührt oder die Informationen würden zu einer Schädigung der Umwelt beitragen. Schließlich bleibt festzuhalten, daß sämtliche Daten, die Gegenstand eines Vorverfahrens oder eines gerichtlichen Verfahrens sind, schon wegen des Schutzes dieser Verfahren zeitweise nicht dem Informationsanspruch unterliegen."

Diesen Anregungen ist das Umweltministerium durch eine (vorläufige) Verwaltungsvorschrift weitgehend gefolgt.

An den kommenden, erwünschten ressortübergreifenden Verhandlungen hoffe ich - auch im Hinblick auf eine Beeinflussung des Bundesrates - bald beteiligt zu werden.

13 Wissenschaft und Kunst

13.1 Hochschulen

13.1.1 Forschungsvorhaben zur Untersuchung der Lebensbedingungen von Vorruheständlern

Eine Universität plant eine Untersuchung der Lebensbedingungen und des subjektiven Befindens von Vorruheständlern. Eine repräsentative Stichprobe läßt sich nur über die Adreßkartei des Arbeitsamts ermöglichen. Versichert wurde, daß die Auswertung keine Zuordnung der Daten zu bestimmten Personen zulasse. Ich habe keine Bedenken gegen das Vorhaben geäußert, jedoch darauf hingewiesen, daß die Anschriften der Probanden und die Untersuchungsergebnisse in getrennten, voneinander unabhängigen Dateien zu führen und so anzulegen sind, daß eine Deanonymisierung (Zuordnung zu einer Person) nicht möglich ist.

13.1.2 Anerkennung der Gleichwertigkeit von Bildungsabschlüssen

Gemäß Art. 37 Abs. 1 Satz 1 Einigungsvertrag (EVertr) gelten die in der DDR erworbenen schulischen, beruflichen und akademischen Abschlüsse weiter. Die in den neuen und den alten Bundesländern abgelegten Prüfungen und Befähigungsnachweise stehen jedoch nur dann einander gleich und verleihen nur dann die gleichen Berechtigungen, wenn sie gleichwertig sind. Die Gleichwertigkeit wird auf Antrag von der zuständigen Stelle geprüft und festgestellt (Art. 37 Abs. 1 Sätze 2 u. 3 EVertr).

In Sachsen ist das Verfahren zur Feststellung der Gleichwertigkeit in der "Bekanntmachung des Sächsischen Staatsministeriums für Wissenschaft und Kunst über die Gleichwertigkeit von Bildungsabschlüssen" vom 30. Januar 1991 geregelt. Mit dem Antrag auf Feststellung sind danach eine Reihe von Unterlagen, nämlich Kopien der Diplomurkunde und des Abschlußzeugnisses, bei bestimmten Abschlüssen Kopien der Urkunde über die Verleihung der Berufsbezeichnung und Nachweise über die Berufstätigkeit (insbesondere Sozialversicherungs-ausweis, Arbeitsvertrag, Arbeitgeberbescheinigung) sowie bei Namensänderung deren Nachweis beizufügen. Es werden also zahlreiche Daten der Antragsteller verarbeitet.

Nach der Rechtsprechung des Bundesverfassungsgerichts erfordert der Eingriff in das Grundrecht auf informationelle Selbstbestimmung nicht nur eine Regelung durch eine Rechtsvorschrift, also ein Gesetz, eine auf einem Gesetz beruhende Rechtsverordnung oder eine Satzung. (Die hier vorliegende Verwaltungsvorschrift genügt also nicht.) Diese Rechtsvorschrift soll aber auch "normenklar" sein, d.h. möglichst bereichsspezifisch ausgestaltet sein. Der Gesetzgeber soll sich nämlich für den konkret zu regelnden, engen Sachbereich Gedanken darüber machen, ob und wieweit er es für verhältnismäßig hält, in das betroffene Grundrecht einzugreifen.

Die Datenerhebung war hier zwar mit dem SächsDSG vereinbar, da für die Aufgabenerfüllung erforderlich. Das SächsDSG gilt jedoch nur subsidiär; der datenschutzrechtlich bessere Weg wäre eine bereichsspezifische Regelung gewesen.

Meinem Hinweis auf die Erforderlichkeit einer gesetzlichen Regelung hielt das Staatsministerium für Wissenschaft und Kunst entgegen, eine Datenerhebung liege nicht vor, da hierzu ein zielgerichtetes Tätigwerden des Ministeriums erforderlich sei. Dies sei nicht der Fall, wenn die personenbezogenen Daten wie hier unaufgefordert zugeleitet werden bzw. wenn der Antragsteller sich mit Bezugnahme auf die Bekanntmachung des Staatsministeriums vom 30.1.1992 von sich aus an das Ministerium wendet. Zwar liege eine Speicherung der Daten vor, diese sei aber mit § 12 Abs. 1 SächsDSG vereinbar.

Dieser Argumentation bezüglich der Erhebung habe ich widersprochen. Gemäß § 3 Abs. 1 Nr. 1 SächsDSG ist Erheben das Beschaffen personenbezogener Daten. Der Begriff "Beschaffen" setzt nicht eine besondere, zielgerichtete Aktivität der beschaffenden Stelle voraus, durch die sie Kenntnis von den Daten erhält oder Verfügung über sie begründet. Ein Erheben von Daten liegt vielmehr nur dann nicht vor, wenn jemand der Behörde völlig unaufgefordert seine personenbezogenen Daten außerhalb eines vorgesehenen Verfahrens zusendet. Hier war die Situation jedoch anders. Zwar liegt es in der Hand des Einzelnen, ob er einen Antrag stellt. Das weitere Verfahren wird ihm jedoch vom Staatsministerium vorgegeben. So regelt § 4 der Bekanntmachung vom 30. Januar 1992, welche Unterlagen er beizufügen hat. Die Aktivität der Behörde liegt also im Erfragen der personenbezogenen Daten. In einer solchen "Erfragung" ist eine Datenerhebung zu sehen.
Das Ministerium verkennt hier grundlegende juristische Begriffe und meint, Verwaltung sei eine freiwillige und unverbindliche Angelegenheit, wenn sie auf Antrag des Bürgers tätig wird.

Daß nicht allein dadurch, daß der Bürger von sich aus an die Behörde herantritt, indem er einen Antrag stellt, eine Erhebung begrifflich ausgeschlossen ist, wird auch dadurch deutlich, daß andernfalls in einem wesentlichen Teil moderner Staatstätigkeit, der Leistungsverwaltung, in der in aller Regel ein Antrag für die Gewährung von Leistungen erforderlich ist, eine Datenerhebung im rechtlichen Sinne nicht stattfinden würde; ein merkwürdiges Ergebnis!

Aber selbst wenn das SMWK Recht hätte, wäre dennoch eine bereichsspezifische Regelung erforderlich, da in jedem Fall eine Speicherung von Daten vorliegt.
Überdies: Die Verweigerung einer Leistung kann den Bürger ebenso hart treffen wie ein Eingriff. Deshalb ist auch Leistungsverwaltung hoheitsrechtliche Tätigkeit. Daten bei der Behörde sind in diesem Zusammenhang immer "erhoben".

13.1.3"Schwarze Listen" des Wissenschaftministeriums

Im November 1992 versandte das Sächsische Staatministerium für Wissenschaft und Kunst (SMWK) Listen an die Rektoren sämtlicher Hochschulen des Freistaates Sachsen, in denen 884 Hochschullehrer und sonstige Hochschulmitarbeiter aufgeführt worden waren, für die, wie es hieß, "mangels persönlicher Eignung ein Kündigungsverfahren vom SMWK eingeleitet" worden sei. Dabei handelte es sich zum einen um Bedienstete, denen *laut Liste* - wegen ihrer Zugehörigkeit zum MfS bzw. wegen Verstoßes gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit (vgl. Anlage I Kap. XIX Sachgebiet A Abschn. III Nr. 1 Abs.5 Einigungsvertrag) - gekündigt worden war (473 Personen) oder gekündigt werden sollte (222 Personen). Auf den Listen waren außerdem 189 Personen aufgeführt, deren Arbeitsverhältnisse, wiederum laut Liste, auf sonstige Weise beendet worden war (Auflösungsvertrag, Bedarfskündigung etc.). Die Listen wurden mit einem Schreiben des Sächsischen Staatsministers für Wissenschaft und Kunst versandt, in dem dieser darauf hinwies, daß eine Wiedereinstellung dieser Personen an einer sächsischen Hochschule grundsätzlich ausgeschlossen sei.

Dieser Vorgang wurde von mir nach § 26 Abs. 1 SächsDSG *förmlich beanstandet*, weil die Listenversendung *zur Aufgabenerfüllung des SMWK nicht erforderlich gewesen war* (§ 31 Abs. 1 SächsDSG). Dies wäre nur dann der Fall gewesen, wenn sie zur rechtmäßigen Aufgabenerfüllung geeignet und unter mehreren möglichen und geeigneten Maßnahmen diejenige gewesen wäre, die den Einzelnen am wenigsten beeinträchtigte (Verhältnis mäßigkeit).
Es war nicht erforderlich, die Listen zu versenden, denn sie waren nicht geeignet, eine gesetzliche Aufgabe des Ministeriums oder der Hochschulen zu erledigen. Es stellte sich nämlich heraus, daß bei weitem nicht sämtliche Personen auf den Listen aufgeführt waren, die der Minister für "persönlich ungeeignet" hielt. Alle, die - in Kenntnis eigener Belastung - vor dem 30.6.1992 aus dem Hochschuldienst ausgeschieden sind, waren nicht vermerkt. Die Liste war demgemäß nicht geeignet, abschließend Auskunft über die Einstufung eines möglichen Bewerbers als "persönlich ungeeignet" zu geben. Stand ein Bewerber nicht auf der Liste, konnte ein Hochschulrektor nicht davon ausgehen, daß dieser aus der Sicht des Ministers im genannten Sinne "persönlich geeignet" war.

Der Minister für Wissenschaft und Kunst hat daraufhin versucht, die *Erforderlichkeit* der Listenversendung mit dem Zeitdruck zu begründen, unter dem die Hochschulverwaltung bei den vielen anstehenden Stellenneubesetzungen gestanden habe. Eine Wiedereinstellung belasteter Hochschulmitarbeiter sei unter diesen Umständen ohne die Versendung der Listen nicht wirksam zu verhindern gewesen.

Auch aus diesem Gesichtspunkt läßt sich jedoch, sieht man genauer hin, die datenschutzrechtlich notwendige Erforderlichkeit der Listenverwendung nicht herleiten.

Denn es hätte auch auf eine andere Weise verhindert werden können, daß als "persönlich ungeeignet" eingestufte Hochschulmitarbeiter aus Unkenntnis dieser Einstufung an einer anderen sächsischen Hochschule wieder eingestellt werden; und zwar auf eine Weise, die nicht nur weniger in das Grundrecht auf informationelle Selbstbestimmung eingegriffen hätte, sondern auch wesentlich schneller und effektiver gewesen wäre:

Die das Recht auf informationelle Selbstbestimmung am wenigsten beeinträchtigende Lösung wäre die rechtzeitige Versendung der Bescheide nach § 81 Sächsisches Hochschulerneuerungsgesetz (SHEG) gewesen. Danach sollten die Betroffenen nach Abschluß des Verfahrens zur Erneuerung des wissenschaftlichen und künstlerischen Personals einen Bescheid des Staatsministers für Wissenschaft und Kunst über den Ausgang der Überprüfung erhalten. Wären diese Bescheide rechtzeitig erteilt worden, hätte sie der jeweilige Bewerber bei seiner Bewerbung vorlegen können. Dazu stand eine Zeit von insgesamt 18 Monaten zur Verfügung.
Eine weitere Möglichkeit wäre gewesen, daß sich die Rektoren der Hochschulen bei jeder konkreten Bewerbung bei derjenigen Hochschule über den Abschluß des Überprüfungsverfahrens erkundigten, an der der Bewerber zuvor beschäftigt war. So wurde es vor und nach der Existenz der Listen mit Erfolg praktiziert.
Schließlich hätten die Listen auch - als zulässige interne Maßnahme - ausschließlich beim SMWK geführt werden können. Das SMWK hätte die Listen bei sich verwahren und Anfragen der Rektoren zu Personen, die an der jeweiligen Hochschule eingestellt werden sollten, im konkreten Fall beantworten können. Dieses "Listenabfrageverfahren" hätte verhindert, daß bei den Rektoren der Hochschulen unzulässigerweise Daten "auf Vorrat" gesammelt würden (nämlich nur für den Fall, daß sich eine Person trotz berechtigter und bestandskräftiger Kündigung bei einer anderen Hochschule in Sachsen bewirbt). Im übrigen wäre das "Listenabfrageverfahren" schon deswegen nicht zeitaufwendiger gewesen als die Versendung der Listen, weil diese unvollständig bzw. falsch waren und deshalb zusätzliche Nachforschungen der Rektoren der Hochschulen bzw. Änderungen der Listen durch das SMWK erforderlich waren. Stattdessen erhielt jeder Rektor mit den Listen besonders schutzwürdige, zudem verfahrensrechtlich ungesicherte persönliche Daten, die er nicht benötigte, weil sich ein Großteil der auf den Listen aufgeführten Personen an der jeweiligen Hochschule - auch in Zukunft - nicht bewirbt.

Im Ergebnis haben die Listen in den Verwaltungen der Hochschulen eher verwirrt als geholfen.

Die überschaubare 'Gemeinde' der Hochschullehrer hingegen hat die Listen - dies ist mir aus Einzelgesprächen bekannt - mit großen Interesse zur Kenntnis genommen.

Die Listenversendung hat ferner gegen die Rechtsschutzgarantie des Art. 19 Abs 4 GG verstoßen. Diese ist eine wesentliche Säule des Rechtsstaats und sieht vor, dass jede in Grundrechte eingreifende Entscheidung vor unabhängigen Gerichten anfechtbar sein muß. Aus der Rechtsschutzgarantie ergeben sich auch Vorwirkungen auf die

Gestaltung des Verwaltungsverfahrens, das der gerichtlichen Kontrolle vorangeht.

Das SMWK hat durch seine Vorgehensweise einem großen Teil der auf den Listen aufgeführten Personen die Erlangung effektiven Rechtsschutzes unmöglich gemacht, da ihnen der Ausgang des Überprüfungsverfahrens in Form der gesetzlich vorgesehenen Entscheidung des Ministers entgegen § 81 SHEG nicht rechtzeitig mitgeteilt, gleichwohl aber die Möglichkeiten ihres beruflichen Fortkommens (Art. 12 Abs. 1 Satz 1 GG) beeinträchtigt wurden.

Die Aufnahme in die Liste ersetzt keinesfalls den rechtsmittelfähigen Bescheid, sondern war als verwaltungsinterne Maßnahme ohne unmittelbare Außenwirkung ausgestaltet, die gerichtlich nicht nachprüfbar war und sein sollte. Ein solches vor dem Betroffenen geheimgehaltenes Informations-System mit verwaltungsinternen verbindlichen Anweisungen, die zu einem Eingriff in ein Grundrecht führen, widerspricht dem Rechtsstaat zutiefst. Effektiver Rechtsschutz im Sinne des Art. 19 Abs. 4 GG wäre nur gewährleistet gewesen, wenn die Betroffenen die Möglichkeit gehabt hätten, gegen den der Listenversendung zugrundeliegenden Bescheid nach § 81 SHEG vorzugehen. Ein solcher Bescheid lag zumindest denjenigen Personen nicht vor, die auf den Listen standen, obwohl deren Beschäftigungsverhältnisse entweder noch gar nicht gekündigt waren oder aus einem ganz anderen Grund als dem im Einigungsvertrag (s. o.) genannten gelöst wurden (411 Fälle).

Außerdem hat der Minister durch die Listenversendung auch seine Fürsorgepflicht als Arbeitgeber verletzt: Zur grundsätzlich bestehenden Beschäftigungspflicht des Arbeitgebers bis zum Zugang der Kündigungserklärung gehört auch die Pflicht, alles zu unterlassen, was den Arbeitnehmer, gegenüber dem kein Recht zur Kündigung der Arbeitsverhältnisse besteht, hindern könnte, bei demselben Arbeitgeber an anderer Stelle wieder eingestellt zu werden.

Darüber hinaus ist bei der Erstellung der Listen die Formvorschrift des § 31 Abs. 7 SächsDSG nicht beachtet worden. Hiernach hätte die automatisierte Verarbeitung von Daten der Beschäftigten nur im Benehmen mit dem Datenschutzbeauftragten eingeführt, angewendet, geändert oder erweitert werden dürfen. Dazu hätte das SMWK den Sächsischen Datenschutzbeauftragten vorher *unterrichten* müssen. Das hat das Ministerium jedoch versäumt.

Schließlich wurden vom SMWK keine ausreichenden Maßnahmen getroffen, um die in den Listen enthaltenen Daten zu *sichern* (§ 9 SächsDSG). Die Listen wurden ohne konkrete Sicherungsmaßnahmen verschickt, so daß fast schon vorprogrammiert war, daß die Listen in weitere Hände als in die der Rektoren der Hochschulen gelangten. Erst nach meiner förmlichen Beanstandung gingen den Hochschulrektoren konkrete Hinweise des Ministers zur Datensicherung zu.

Im Auftrag des Sächsischen Landtags habe ich zu dem Vorgang am 4.3.1993 berichtet (Drucksache Nr. 1/2948).

13.2 Denkmalschutzgesetz

Zum von der Staatsregierung vorgelegten *Entwurf* eines "Gesetzes zum Schutz und zur Pflege der Kulturdenkmale im Freistaat Sachsen" mußte ich das Sächsische Staatsministerium des Innern darauf aufmerksam machen, daß ich entgegen § 15 Abs. 5 Satz 2 der Geschäftsordnung der Sächsischen Staatsregierung nicht beteiligt worden war, obwohl der Umgang mit personenbezogenen Daten berührt ist.
Auch zum *Inhalt* des Gesetzentwurfs ergab sich in einigen Punkten Anlaß zu kritischen Anmerkungen. § 10 Abs. 1 und 2 regeln die Aufnahme der Kulturdenkmale in Listen (Kulturdenkmallisten). Gemäß § 3 Abs. 1 ist der Eigentümer von der Eintragung zu unterrichten. Die Anforderungen, die an eine verfassungsrechtlich einwandfreie normenklare Regelung der Datenerhebung zu stellen sind, sind nicht erfüllt. Es muß sehr viel genauer festgelegt werden, unter welchen Voraussetzungen welche Daten in die Kulturdenkmallisten aufgenommen werden können. Nicht ausreichend ist es, das Nähere - wie in Absatz 5 vorgesehen - durch Verwaltungsvorschriften regeln zu lassen, da jede Datenerhebung auf Gesetz beruhen muß.
Erhebliche Bedenken ergeben sich gegen § 10 Abs. 3 Satz 3, wonach "jedermann" die Einsicht in die Kulturdenkmallisten gestattet ist. Einschränkungen macht Satz 4 bei Eintragungen über *bewegliche* Kulturdenkmale und über Zubehör, die nur vom Eigentümer und den sonstigen dinglich Berechtigten und von den von ihnen ermächtigten Personen eingesehen werden dürfen. Diese Unterscheidung ist nicht sachgerecht, da auch bei unbeweglichen Kulturdenkmalen ein berechtigtes Interessen des Eigentümers daran besteht, daß nicht "jedermann" seine personenbezogenen Daten zugänglich gemacht werden.
Dagegen kann auch nicht eingewandt werden, wie es das Sächsische Staatsministerium des Innern versucht hat, eine Verarbeitung personenbezogener Daten sehe das Gesetz nicht vor. In den Listen seien weder personenbezogene Daten enthalten noch ließen diese Rückschlüsse darauf zu. Es sei nur die Bezeichnung des Objekts und sein Standort eingetragen.
Personenbezogene Daten sind nämlich § 3 Abs. 1 SächsDSG Einzelangaben über persönliche und sachliche Verhältnisse einer *bestimmten* oder *bestimmbaren* natürlichen Person. Zur Vorbereitung der Eintragung erhebt die Denkmalschutzbehörde personenbezogene Daten bestimmter Personen, nämlich der jeweiligen, der Behörde namentlich bekannten Eigentümer, und speichert sie. Auch die folgende Eintragung in die Kulturdenkmallisten ist eine Speicherung, und zwar wiederum eines Datums einer bestimmten Person, da die Behörde den Eigentümer namentlich kennt.
Die Listen sollen jedermann zugänglich sein. Sobald ein Bürger sie einsieht, liegt eine Übermittlung der Daten gemäß § 3 Abs. 2 Nr. 5 SächsDSG vor. Für ihn sind es zwar, da der Eigentümer in der Liste nicht genannt wird, keine Einzelangaben über eine bestimmte, jedoch über eine bestimmbare Person, da der Personenbezug durchaus auf vielfältige Weise herstellbar ist. Das gilt erst recht für andere öffentliche Stellen (als die

Denkmalschutzbehörden), die diese Listen verwenden.
Wünschenswert wäre also eine klare bereichsspezifische Regelung dieser Datenverarbeitung im Denkmalschutzgesetz gewesen. Da eine solche Regelung fehlt, muß auf das subsidiär anzuwendende Sächsische Datenschutzgesetz zurückgegriffen werden. Danach ist die Datenverarbeitung zulässig, wenn von dem betroffenen Eigentümer eine § 4 Abs. 2 SächsDSG entsprechende Einwilligung eingeholt wird. Da eine Datenverarbeitung hier jedoch auch *gegen* den Willen des Eigentümers möglich sein soll, ist dieser Weg verbaut. Es müssen also die Voraussetzungen erfüllt sein, die das Sächsischen Datenschutzgesetz für den Fall des Fehlens einer Einwilligung aufstellt. Man wird bejahen können, daß die Erhebung der Daten (§ 11 SächsDSG) für die Aufgabenerfüllung einer Denkmalbehörde erforderlich ist.
Das gleiche gilt für die Speicherung und die Eintragung der Daten in die Listen, da sie zur Aufgabenerfüllung erforderlich sind, die Daten nicht in unzulässiger Weise erhoben wurden und die Eintragung für die Zwecke erfolgt, für die sie erhoben wurden (§ 12 Abs. 1 SächsDSG).
Problematisch wird es allerdings bei der Einsichtnahme in die Listen durch "jedermann". Eine solche Übermittlung von Daten an nicht-öffentliche Stellen ist nur unter den Voraussetzungen des § 15 SächsDSG zulässig.
Nach meiner Auffassung ist es zur Erfüllung der Aufgaben der Denkmalschutzbehörde *nicht erforderlich*, daß *jeder* Einsicht in die Kulturdenkmallisten enthält. Die Voraussetzungen nach § 15 Abs. 1 Nr. 1 SächsDSG, der ersten der beiden möglichen Erlaubnistatbestände dieser Vorschrift, sind daher nicht erfüllt.
Aber auch § 15 Abs. 1 Nr. 2 SächsDSG kann die Zulässigkeit der Übermittlung nicht begründen. Denn der Betroffene hat ein schutzwürdiges Interesse daran, daß die Übermittlung unterbleibt. Deshalb ist sie nicht zulässig.
Bei beweglichen Sachen geht im übrigen das Denkmalschutzgesetz selbst in § 10 Abs. 3 davon aus, daß ein solches schutzwürdiges Interesse des Eigentümers vorliegt, indem es nur bestimmten Personen die Einsichtnahme in die Kulturdenkmallisten gestattet. Zwar ist der Argumentation des SMI zuzustimmen, daß im Hinblick auf Diebstahlgefahr bei beweglichen Sachen das Interesse stärker ist als bei Immobilien. Aber auch bei diesen können Eigentümer durchaus ein schutzwürdiges Interesse daran haben, daß die Daten nicht jedem zugänglich sind, denn Besitz- und Eigentumsverhältnisse, Art der Nutzung, Denkmaleigenschaft etc. sind der grundrechtlich geschützten Privatsphäre zuzurechnen, es sei denn, es besteht ein unabweisbares - bislang auch nicht ansatzweise erkennbares - Bedürfnis nach Veröffentlichung.

Man muß wissen, daß der Neid - in früheren Zeiten klarer erkannt als heute - eine Triebfeder für sozial abträgliches Verhalten, also schlicht ein *Laster* ist.

Am 17. März 1993 ist der Entwurf - ohne daß meine Anregungen berücksichtigt worden wären - Gesetz geworden. Das mag auch daran gelegen haben, daß ich zu spät informiert wurde. An meiner Auffassung halte ich fest.

14 Datensicherheit

14.1 Datensicherheit durch technische und organisatorische Maßnahmen

Datensicherheit dient nicht nur dazu, Daten Betroffener vor Mißbrauch, Verfälschung oder Verlust zu schützen sind, sondern gewährleistet im öffentlichen Interesse den Dienstbetrieb. Vom Gesetzgeber werden für jede Verarbeitung personenbezogener Daten Datensicherungsmaßnahmen gefordert. Diese sollen mit technischen Mitteln verhindern, daß

- Datenmißbrauch,
- Datenverfälschungen,
- Datenverluste,
- Datenzerstörungen oder
- Datenentwendungen

eintreten können. Datensicherheit ist Voraussetzung für praktizierten Datenschutz. Sie wird oft als die "technische Seite" des Datenschutzes bezeichnet. Die Aufgabe, Datensicherheit zu gewährleisten, ist nicht neu; heute muß jeder Behördenleiter, jedes Rechenzentrum zum Schutz der betroffenen Menschen darauf achten, daß Datenbestände ausreichend geschützt sind und Programme ordnungsgemäß "abgearbeitet" werden können.

Das SächsDSG sieht in § 9 die technisch-organisatorischen Maßnahmen vor, die für eine Verarbeitung personenbezogener Daten durch öffentliche Stellen beachtet werden müssen. Das Gesetz verlangt einen angemessenen und vertretbaren Aufwand für die Datensicherheit, der sich am Schutzbedarf der Daten zu orientieren hat und der von der "Sensibilität" der Daten, d.h. von der Tiefe des Eingriffs in das Persönlichkeitsrecht, abhängt. Der Schutzbedarf für "öffentliche Daten", wie z. B. die Anschrift einer Person oder deren Telefonnummer, ist im allgemeinen gering.
Dagegen sind für Daten über soziale und finanzielle Verhältnisse oder über religiöse und politische Anschauungen deutlich strengere Sicherheitsmaßnahmen vorzusehen.

Manipulationen, Transformationen und Gefährdungen von Daten bei ihrer Bearbeitung sind vielfältig möglich. Deshalb kann der Gesetzgeber keine konkreten Datensicherungsmaßnahmen vorschreiben.

Neben Behördenleitern und Vorgesetzten ist jeder EDV-Anwender selbst dafür verantwortlich, unter Beachtung der Forderungen des § 9 SächsDSG spezielle Sicherheitsvorkehrungen vorzusehen und einzuhalten. Dabei ist es belanglos, ob es sich um eine größere EDV-Anlage in einem Rechenzentrum oder "nur" um einen PC handelt. Der Anwender muß - nach Maßgabe der gesetzlichen Vorschriften - selbst entscheiden, welche personellen, technischen und organisatorischen Sicherungsmaßnahmen für den Schutz der bearbeiteten Daten sinnvoll, zweckmäßig und ausreichend sind. Möglichkeiten dazu können sein:

- Räumliche Abschottung von Anlagen und Anlagenteilen
- Benutzerkontrolle (Identifikation und Authentifikation)
- Unterscheidung verschiedener Zugangsklassen
- zahlenmäßige Begrenzung von Zugriffsversuchen
- Protokollierung einer Datennutzung
- Datenträgerverwaltungssystem
- Einschränkung von Kopiermöglichkeiten
- Verschlüsselung
- Funktionstrennung
- Benutzerverwaltung

Die technischen und organisatorischen Maßnahmen gemäß § 9 SächsDSG werden in den *"10 Geboten der Datensicherheit"* zusammengefaßt:

1. *Zugangskontrolle:*
   Unbefugten ist der Zugang zu Rechenzentren sowie zu allen Räumen, in denen sich EDV-Geräte befinden, zu verwehren.
2. *Datenträgerkontrolle:*
   Datenträger dürfen nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.
3. *Speicherkontrolle:*
   Unbefugte Eingabe, Kenntnisnahme, Veränderung oder Löschung gespeicherter Daten ist zu verhindern.
4. *Benutzerkontrolle:*
   Datenverarbeitungssysteme dürfen nicht mit Hilfe von Einrichtungen zur Datenübertragung unbefugt benutzt werden können.
5. *Zugriffskontrolle:*
   Es ist zu gewährleisten, daß Nutzungsberechtigte ausschließlich auf diejenigen Daten zugreifen können, für die sie eine Zugriffsberechtigung besitzen.
6. *Übermittlungskontrolle:*
   Es muß überprüft werden können, wann und von wem Daten abgerufen oder an wen sie (selbständig) übermittelt werden.
7. *Eingabekontrolle:*
   Nachträglich muß kontrollierbar sein, wer wann welche Daten in ein Datenverarbeitungssystem eingegeben hat.

8. *Auftragskontrolle:*
   Daten, die im Auftrag verarbeitet werden, dürfen nur gemäß Weisung des Auftraggebers verarbeitet werden.
9. *Transportkontrolle:*
   Es ist zu verhindern, daß bei Datenübertragungen sowie beim Transport von Datenträgern diese unbefugt gelesen, kopiert, verändert oder gelöscht werden können.
10. *Organisationskontrolle:*
    Die innerbetriebliche Organisation muß so gestaltet werden, daß sie den Anforderungen der Datensicherheit gerecht wird.

Automatisierte Datenverarbeitung muß jederzeit die *Kontrollierbarkeit* und die *Nachvollziehbarkeit* der Bearbeitungsprozesse gewährleisten. Hersteller und Anwender müssen dafür sorgen, daß Hard- und Software-Systeme sowie Anwenderverfahren kontrollierbar bleiben. Angesichts der zunehmenden Komplexität der Systeme (Vielzahl von PC, Vernetzung, Informationssysteme) sind dies hohe Anforderungen.
Die Schutzmaßnahmen sind dann ausreichend, wenn sie in ihrer Gesamtheit eine ausreichende Gewähr gegen Beeinträchtigungen schutzwürdiger Belange Betroffener bieten.
Als Orientierungshilfen stellt meine Behörde auf Anforderung folgende Merkblätter, Hinweise und Formulare zur Verfügung:

- Hinweise zu den Aufgaben eines internen Datenschutzbeauftragten öffentlicher Stellen (siehe Nr. 16.1.2)
- Empfehlungen zur Paßwortgestaltung (siehe Nr. 16.3.4)
- Formular zum Führen eines Dateien- und Geräteverzeichnisses gemäß § 10 Sächs-DSG (siehe Nr. 16.3.3)

14.1.1 Einzelfragen

Verstoß gegen die Datensicherheit (§ 9 Abs. 2 Nr. 2 SächsDSG)

Täglich fallen in der Verwaltung große Mengen Papier an, die zu einem späteren Zeitpunkt nicht mehr benötigt werden. Diese Unterlagen müssen ordnungsgemäß vernichtet werden.
Im November 1992 teilte ein Journalist der Bildzeitung meiner Behörde telefonisch mit, daß hinter dem Dienstgebäude des Landesamtes für Finanzen in Leipzig auf dem Gehweg mehrere Müllsäcke mit personenbezogenen Unterlagen stünden. Ich fuhr sofort dorthin und sah, daß vier Müllsäcke mit Bezügeabrechnungen von Lehrern, also mit teilweise sensiblem Inhalt, für jedermann zugänglich dort gelagert waren.
Der Dienststellenleiter teilte mir mit, daß jeder Bedienstete mündlich angewiesen sei, personenbezogene Daten, die nicht archiviert werden, zu sammeln und in den im Keller aufgestellten Reißwolf zu stecken; Zugang zum Aktenvernichtungsraum habe nur ein kleiner Kreis von Beschäftigten und eine Reinigungsfirma. Wer die Schriftstücke aus

dem Aktenvernichtungsraum entfernt hatte, konnte nicht aufgeklärt werden. Der - für Datenschutz und Datensicherheit aufgeschlossene und problembewußte - Behördenleiter reagierte sofort: Er instruierte die Belegschaft, legte persönliche Verantwortlichkeiten fest und organisierte die ordnungsgemäße Papiervernichtung.

Dieser Vorfall ist Anlaß, Organisation und Durchführung der Entsorgung von Datenträgern im folgenden grundsätzlich zu behandeln.

14.1.2 Entsorgung von Datenträgern

Zur Entsorgung werden Datenträger gesammelt, gelagert, transportiert und vernichtet. Der Gesetzgeber fordert in § 9 SächsDSG für Datenträger mit *personen*bezogenen Daten geeignete technisch-organisatorische Schutzmaßnahmen. Die Datenträger (Magnetplatten, Disketten, Magnetbänder, Carbonbänder, Computerlisten, Einzelausdrucke), aber auch sonstige Schriftstücke mit personenbezogenen Daten sollen vor unberechtigtem Zugriff bzw. unbefugter Kenntnisnahme geschützt werden. Während der Verarbeitung von Daten im EDV-Bereich wird der Schutz meist durch aufwendige technische und organisatorische Maßnahmen realisiert. Das muß bei der Entsorgung vereinfacht werden. Eine sichere Entsorgung von Schriftstücken ist dabei besonders wichtig, weil deren Inhalt unmittelbar gelesen und mißbraucht werden kann.

Unterlagen (Akten, Urkunden, Einzelschriftstücke, Tonträger u. a.) sind grundsätzlich - jedoch spätestens 30 Jahre nach ihrer Entstehung - dem zuständigen Archiv anzubieten. Es entscheidet im Benehmen mit der anbietenden öffentlichen Stelle innerhalb von sechs Monaten über die Archivwürdigkeit der Unterlagen. Wird eine solche bejaht, hat das Archiv die Unterlagen zu übernehmen; anderenfalls kann die öffentliche Stelle die Unterlagen vernichten (vgl. Nr. 5.8). Eine Einteilung in Sicherheitsstufen nach DIN 32 757 (Deutsche Industrie-Norm über das Vernichten von Informationsträgern) ist nicht notwendig, denn das Datenschutzrecht kennt keine Unterscheidung personenbezogener Daten nach "Sicherheitsstufen". Der mit einer Klassifizierung verbundene Aufwand wäre - ausgenommen bei wirklich geheimen Unterlagen - auch unerträglich.

Vor der Entsorgung magnetischer Datenträger sollte durch sicheres Löschen das Altdatenrisiko beseitigt werden. Die *üblichen Löschfunktionen* der Betriebssysteme (z. B. DELETE, ERASE) sind dafür *nicht ausreichend.* Sie ändern lediglich die Einträge der Inhaltsverzeichnisse. Die Daten selbst sind physisch noch auf dem Datenträger vorhanden und ihre Lesbarkeit kann mittels einfacher 'Tools' (Softwarewerkzeuge) wiederhergestellt werden. Mit speziellen Löschprogrammen oder mit Magnetfeldlöschgeräten kann dagegen eine tatsächliche Datenlöschung erfolgen. Eine sichere Möglichkeit zur Entsorgung ist die physische Vernichtung (z. B. shreddern). Der Vernichtungsvorgang ist revisionsfähig zu protokollieren. Die Protokolle sind aufzubewahren.

Bei der Entsorgung sollten folgende Forderungen beachtet werden:
- Sicherungsmaßnahmen müssen lückenlos von der Sachbearbeitung bis zur Aktenvernichtung erfolgen und durch Dienstanweisungen geregelt werden .
- Getrenntes Sammeln von Datenträgern mit schutzwürdigem und nicht schutzwürdigem Inhalt ist nicht zu empfehlen (Gefahr der Verwechslung; zu hoher Aufwand).
- Eine Aktenvernichtung sollte möglichst dort erfolgen, wo die Sacharbeit durchgeführt wird (Aktenvernichter in unmittelbarer Nähe). Das ist die sicherste und zugleich preiswerteste Lösung!
- Sammlung, Lagerung und Transport des "Vernichtungsgutes" in geschlossenem Behälter.
- Vernichtungsprotokoll erstellen
- Bei Fremdentsorgung ist der Auftraggeber sorgfältig auszuwählen.

14.2 Digitale Telekommunikationsanlagen - ISDN

Ende des Jahres 1992 wurde ein Telekommunikations-Anlagenverbund zwischen den Staatsministerien und dem Landtag installiert und in Betrieb genommen. Er soll die Kommunikationsmöglichkeiten verbessern. Die dafür zugrunde gelegte ISDN-Technik (*I*ntegrated *S*ervices *D*igital *N*etwork) ermöglicht neben dem normalen Telefonieren weitere Anwendungen wie Text-, Bild- oder Datenübertragung. Außerdem sind Leistungsmerkmale wie Rufweiterleitung, Rufumleitung und Rückruf möglich. Durch Nutzung von Querverbindungen können Telefongebühren eingespart werden. Der Einsatz einer solchen ISDN-Anlage ist datenschutzrechtlich deshalb bedeutsam, weil für jedes Telefonat ein personenbezogener Datensatz angelegt wird. Dieser enthält Aussagen über Zeitpunkt und Dauer des Gesprächs sowie Angaben zu den Gesprächsteilnehmern.

Den Sächsischen Staatsministerien und deren Hauptpersonalräten habe ich zum Betrieb einer solchen ISDN-Telefonanlage meine Auffassung wie folgt dargelegt:
Die Einrichtung einer solchen Anlage ist aus datenschutzrechtlicher Sicht, insbesondere bei der Erfassung von Privatgesprächen, nicht unproblematisch, zumal die umfassende Speicherung von Gesprächsdaten (wer hat wann mit wem wie lange telefoniert) eine Verhaltens- oder Leistungskontrolle der Bediensteten ermöglicht. Sowohl § 75 Abs. 3 Nr. 17 Bundespersonalvertretungsgesetz als auch § 80 Abs. 3 Nr. 16 des Sächsischen Personalvertretungsgesetzes setzen dazu die Mitbestimmung des Personalrates voraus. TK-Anlagen dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und von wem sie ausgewertet werden.

Die Tatsache, daß ein Behördenbediensteter privat mit einem bestimmten Dritten telefoniert, der aufgrund der gespeicherten Zielnummer durch den Dienstherrn (möglicherweise) identifizierbar ist, kann durchaus sensible Bereiche berühren. Den Anforderungen aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz sowie aus Art. 33

Sächsische Verfassung, insbesondere auch des vom Bundesverfassungsgericht anerkannten informationellen Selbstbestimmungsrechts (vgl. auch § 1 SächsDSG), ist deshalb bei der Speicherung und Nutzung der Telefondaten von Privatgesprächen Genüge tun. Auf den Beschluß des Bundesverfassungsgerichts vom 19.12.1991 - 1 BvR 382/85 (NJW 1992, S. 815) - weise ich hin.

Speicherung und Nutzung von Telefondaten bei Privatgesprächen sind aus Sicht des Datenschutzes nur dann zulässig, wenn die Bediensteten darüber informiert sind, unter welchen Voraussetzungen sie den Dienstapparat für private Telefongespräche benutzen können. Der Dienstherr hat insbesondere darauf hinzuweisen, welche Daten im einzelnen gespeichert und welcher Nutzung sie zugeführt werden.

Insbesondere sind folgende Punkte zu beachten:

1. *Allgemeines*
   Zweckbindung: Erfaßte und gespeicherte Gesprächsdaten dürfen nur zur Abrechnung von Gebühren, zur Wirtschaftlichkeitsüberprüfung der Fernmeldeanlagen und für Aussagen über die Verkehrsleistung und Betriebsweise der Anlagen ausgedruckt oder in anderer Weise abgerufen werden.

   Sicherungsmaßnahmen: Zur Sicherstellung der Zweckbindung müssen technische und organisatorische Maßnahmen gemäß § 9 SächsDSG getroffen werden.

2. *Orts- und Nahgespräche*
   Summarische Erfassung: Soweit möglich, können abgehende Orts- und Nahgespräche summarisch nach der Zahl der Gebühreneinheiten je Nebenstelle und Monat erfaßt werden.

   Zweckbindung: Wenn die Führung privater Orts- und Nahgespräche eingeschränkt ist, können private Gespräche zusätzlich gekennzeichnet werden. Ein Ausdruck der dabei gewonnenen Daten ist wiederum auf die oben unter 1 genannten Zwecke beschränkt.

3. *Ferngespräche*
   Einrichtungen zur selbsttätigen Gebührenerfassung erlauben in der Regel die Erfassung folgender Daten:

   - Telefonnummer der rufenden Nebenstelle,
   - Vorwahl und Telefonnummer des angewählten Gesprächsteilnehmers (Zielnummer bei Privatgesprächen in verkürzter Form durch Weglassen der letzten beiden Ziffern),

- Datum und Uhrzeit,
- Gebühreneinheiten und Gebührenbetrag,
- Nummer der Amtsleitung,
- sonstige betriebliche Kennzeichnungen,
- Kennzeichnung als Privatgespräch.

Dienstliche Ferngespräche: Hier kann von den technischen Möglichkeiten zur selbsttätigen Gebührenerfassung ohne Einschränkung Gebrauch gemacht werden. Ein Ausdruck der Daten ist grundsätzlich ebenfalls uneingeschränkt zulässig. Dies schließt nicht aus, daß in besonders gelagerten Fällen (z. B. bei Drogenberatern) aus rechtlichen oder sachlichen Gründen Abweichungen geboten sein können (s. u.).

Erfassung privater Ferngesprächsdaten: Zum Schutze des informationellen Selbstbestimmungsrechts dürfen die letzten beiden Ziffern der Zielnummer nicht gespeichert werden. Damit wäre der Angerufene von einem Unbeteiligten kaum noch zu bestimmen, aber der Anrufer kann sich in der Regel anhand der verfügbaren Ziffern an das Gespräch erinnern. Eine solche verkürzte Speicherung dürfte auch als Beweis für die erbrachte Verbindungsleistung ausreichen, zumal die fehlenden Ziffern für die Zahlungspflicht ohne Bedeutung sind.

Die Bediensteten müssen in geeigneter Weise darauf hingewiesen werden, daß die oben aufgeführten Gesprächsdaten erfaßt, zumindest teilweise ausgedruckt und für Abrechnungszwecke verwertet werden. Andernfalls dürfen private Ferngespräche über dienstliche Fernmeldeanlagen nicht zugelassen werden.

Ausdruck/Zweckbindung: Für Abrechnungszwecke sind in der Regel auszudrucken oder sonst abzurufen und zu verwerten:

- Telefonnummer der rufenden Nebenstelle,
- Datum und Uhrzeit,
- Gebühreneinheiten und Gebührenbetrag,
- Name des Inhabers der Nebenstelle.

Eine Verwertung dieser Daten für andere als Abrechnungszwecke ist auszuschließen.

Ausdruck der Zielnummer: Hat ein Bediensteter Zweifel an der Abrechnung, so ist auf seinen Antrag auch der Ausdruck der übrigen erfaßten Gesprächsdaten einschließlich der verkürzten Zielnummer zulässig.

Sicherung der Ausdrucke:

- Ausdrucke ohne Zielnummer dürfen nur der für die Gebührenrechnung zuständigen Stelle und dem betroffenen Bediensteten zugänglich gemacht werden.
- Ausdrucke mit (verkürzter) Zielnummer dürfen ausschließlich den betroffenen Bediensteten zugänglich gemacht werden.

Versendung und Aufbewahrung in verschlossenem Umschlag ist in beiden Fällen geboten.

Löschung von Daten: Nach Einziehung der Gebühren (wenigstens vierteljährlich) sind die Daten zu löschen und die Ausdrucke zu vernichten, soweit sie nicht den Bediensteten ausgehändigt werden. Die Löschung bzw. Vernichtung hat innerhalb von zwei Monaten nach Ende des Abrechnungszeitraumes zu erfolgen. Können einzelne Abrechnungen nicht rechtzeitig erledigt werden, darf die Frist für die Löschung der Daten und die Vernichtung der Ausdrucke ausnahmsweise überschritten werden. Die Gründe hierfür sind schriftlich festzuhalten.

Daten von *dienstlichen* Telefongesprächen der Personalvertretungen dürfen ohne Einwilligung der betroffenen Bediensteten nur *summarisch* (Summe der Gebühreneinheiten je Nebenstelle) ausgewertet werden. Das gleiche gilt für den gemäß § 23 Abs. 4 Satz 1 SächsDSG unabhängigen Datenschutzbeauftragten und dessen Personal sowie für Bedienstete, die einer besonderen Schweigepflicht unterliegen (z. B. Bedienstete, die im Rahmen einer *freiwilligen* Beratung nach dem Gesetz über den öffentlichen Gesundheitsdienst mit Drogenabhängigen, psychisch Kranken oder Behinderten telefonieren). Auch die anläßlich von Ehe- und Familienberatung oder von AIDS-Beratung geführten Telefonate fallen unter dieses Gebot. Weitere Fälle sind denkbar.

Diesem Personenkreis sollte ein Anschluß zur Verfügung stehen, bei dem generell auf eine *Speicherung der Zielnummer verzichtet* wird.

Aufzeichnungen über Gespräche von Mandatsträgern würden den Schutz der freien Mandatsausübung ins Leere laufen lassen. Um eine angemessene Behandlung dieser "Mandatsgespräche" zu gewährleisten, ließe sich für diese eine der sogenannten "Prominentenschaltung" entsprechende Schaltung einrichten. Darunter ist ein Nebenstellenanschluß zu verstehen, über den durch den installierten Telefoncomputer keinerlei Gesprächsdaten erfaßt werden. Im Vergleich zu den übrigen angeschlossenen Nebenstellen kommt er einem eigenständigen Telefonanschluß gleich. Eine Gebührenkontrolle ist allerdings bei einer "Prominentenschaltung" nicht möglich. Dabei verkenne ich nicht, daß auch die Mandatsträger an die Grundsätze der Wirtschaftlichkeit und Sparsamkeit gebunden sind.

Für Kommunen und nachgeordnete Bereiche der Ministerien habe ich die Grundsätze in einem Merkblatt zum Betrieb digitaler Telekommunikationsanlagen zusammengefaßt (siehe Nr. 16.1.4).

Zum Datenschutz bei internen Telekommunikationsanlagen möchte ich auf die Entschliessung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 hinweisen (siehe Nr. 16.2.4)

14.3 Prüfungstätigkeit

Ich habe das Rechenzentrum der Sächsischen Landesanstalt für Landwirtschaft in Chemnitz- Lichtenwalde (lediglich) im Hinblick auf zu technisch-organisatorische Datenschutzmaßnahmen gemäß § 9 SächsDSG kontrolliert. Dabei wurden folgende *Mängel* bemerkt:

- fehlende Direktverbindung zwischen Rechenzentrum und Polizei/ Feuerwehrstelle
- keine automatische Weiterleitung der Alarmmeldung
- Gefahr des Datenmißbrauchs nach Austausch defekter Festplatten
- Wiederanlaufverfahren war noch nicht getestet
- keine regelmäßige Kontrolle des Datenträgerbestandes
- fehlende bzw. erst in Arbeit befindliche Unterlagen, Beschreibungen für:
    - LAN-Konfiguration
    - Richtlinien für die Übermittlung personenbezogener Daten
    - Planungskonzepte für die Vernetzung in den Ämtern u.ä.
    - Dateien- und Datensatzbeschreibungen
    - Dienstanweisungen
- Reinigung der Räume außerhalb der normalen Arbeitszeit durch eine Fremdfirma ohne Aufsicht und Kontrolle

Maßnahmen und Empfehlungen:

- sichere Alarmerkennung und Weiterleitung der Alarmmeldung durch
    - Ausstattung mit tragbaren Signalgebern für in der Nähe wohnende Mitarbeiter oder
    - Direktverbindung RZ- Polizei / Feuerwehr
    - Einbau von Bewegungsmeldern
- Klausel zur Wahrung des Datengeheimnisses bei Rücknahme defekter Festplatten in den Wartungsvertrag einfügen; Führung eines Entsorgungsprotokolls für die fehlerhaften Festplatten
- Erstellen der Dokumentationen auch im Sinne einer leichteren Kontrolltätigkeit
- Sorgfältigere Archivierung der Datenträger
- Aufsicht und Kontrolle der Reinigung durch Fremdfirma und deren Verpflichtung auf das Datengeheimnis (§ 6 SächsDSG).

Die Ausbildung der Organisationsbeauftragten der 14 Landwirtschaftsämter sollte stärker auf die Belange des Datenschutzes ausgerichtet werden. Alle Mitarbeiter, die sich mit der Verarbeitung personenbezogener Daten befassen, müssen geschult und für den Datenschutz sensibilisiert werden. Nur so kann ein persönliches Verantwortungsgefühl für die Erfordernisse des Datenschutzes und der Datensicherheit entwickelt werden. Dazu habe ich meine Hilfe (bislang ohne Resonanz) angeboten.
Wichtig ist, daß die jeweilige öffentliche Stelle auf kurze, verständliche und unbürokratische Dienstanweisungen zurückgreifen kann, um Datenschutz und Datensicherung sicherzustellen:

- Anlegen und Bearbeiten von Dateien
- Weitergabe von Datenträgern
- Datenarchivierung
- Datenvernichtung

Für den geplanten Einsatz einer ISDN-Nebenstellenanlage ist gemäß § 31 Abs.7 SächsDSG der Datenschutzbeauftragte ins Benehmen zu setzen und die Personalvertretung zu beteiligen. Ich habe Empfehlungen und Hinweise für den Betrieb von Nebenstellenanlagen gegeben, insbesondere bei Verarbeitung personenbezogener Daten durch die Gebühren- Datenerfassung.

Anmerkung:
Ich behalte mir vor, die Organisation des Datenumgangs in der Landwirtschaftsverwaltung 1993 umfassender zu kontrollieren, zumal die Landwirtschaftsämter nicht in die Landratsämter integriert worden sind.

15 Vortrags- und Schulungstätigkeit

Meine Dienststelle hat von Anfang an großen Wert auf die Verbreitung des *Datenschutzgedankens* gelegt und deshalb vielfältige Veranstaltungen durchgeführt oder an solchen teilgenommen.
In Delitzsch haben wir auf Anregung des Hauptamtsleiters des dortigen Landratsamtes am 30. und 31.10.92 eine Fortbildungsveranstaltung für die internen Datenschutzbeauftragten der Landratsämter und kreisfreien Städte abgehalten, die etwa halbjährlich wiederholt werden soll.

Wir haben auch viele Vorträge vor Parlamentariern, Ratsmitgliedern, Landräten, Bürgermeistern, Dezernenten, Amtsleitern, Polizeibeamten, Ärzten, Sozialarbeitern, Fürsorgerinnen, Mitarbeitern von Rechenzentren, vor Belegschaften, Personal- und Betriebsräten, Studenten und anderen gehalten. Dabei haben wir mit unterschiedlichen Bildungsträgern erfreulich zusammenarbeiten können.

Künftig sollen neben den Grundsatzfragen zum Schutz des Persönlichkeitsrechts fachspezifische Schwerpunkte bevorzugt thematisiert werden (z. B. Personalwesen, Soziales, Datensicherheit, Meldewesen).

16 Materialien

16.1 Bekanntmachungen des Sächsischen Datenschutzbeauftragten (SächsABl. S.211)

16.1.1

Bekanntmachung des Sächsischen Datenschutzbeauftragten zu § 35 des Sächsischen Datenschutzgesetzes vom 20. Februar 1992

1. *Verzeichnis der Altdatenbestände*

1.1 Nach § 35 Abs. 2 SächsDSG vom 11. Dezember 1991 (SächsGVBl. S. 401) sind die Personen und Stellen, die die tatsächliche Gewalt über personenbezogene Daten in Akten oder Dateien innehaben, die von ehemaligen staatlichen oder wirtschaftsleitenden Organen, Kombinaten, Betrieben oder Einrichtungen sowie von gesellschaftlichen Organisationen der DDR auf dem Gebiet des Freistaates Sachsen für Zwecke der öffentlichen Verwaltung erhoben oder in anderer Weise verarbeitet wurden, verpflichtet, hierüber ein Verzeichnis dem Sächsischen Datenschutzbeauftragten zuzuleiten.

1.2 Nach § 3 Abs.5 SächsDSG ist eine *Datei*

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann *(automatisierte Datei)* oder
2. eine andere Sammlung personenbezogener Daten, die nach bestimmten Merkmalen geordnet, umgeordnet oder ausgewertet werden kann *(nicht-automatisierte Datei)*.

1.3 Eine *Akte* ist jeder sonstige, amtlichen oder dienstlichen Zwecken dienende Träger personenbezogener Daten; dazu zählen *auch Bild- und Tonträger*, soweit sie nicht Dateien sind (§ 3 Abs. 6 SächsDSG). Ausgenommen sind also Sach- und Schriftwechselakten, die keine personenbezogenen Daten enthalten.

1.4 Gemäß § 35 Abs. 4 SächsDSG sind nicht nur die Akten und Dateien, sondern auch alle *Kopien* hiervon auf Verlangen vorzulegen. Deshalb ist das Verzeichnis auch dann aufzustellen, wenn nur Kopien vorhanden sind.

1.5 Ehemalige staatliche oder wirtschaftsleitende Organe, Kombinate, Betriebe oder Einrichtungen sowie gesellschaftliche Organisationen der DDR *(öffentliche Stellen im Sinne des § 35 Abs. 1 SächsDSG) sind* <u>*insbesondere*</u>

1.5.1 *die staatlichen und kommunalen Behörden und sonstigen Dienststellen* (einschl. Strafvollzugs- und Polizeibehörden), jedoch nicht die Gerichte und die Staatsanwaltschaften

1.5.2 *die Parteien*

Sozialistische Einheitspartei Deutschlands (SED)
Christlich-Demokratische Union (CDU)
Liberal-Demokratische Partei Deutschlands (LDPD)
National-Demokratische Partei Deutschlands (NDPD)
Demokratische Bauernpartei Deutschlands (DBD)
sowie die Nationale Front der DDR (NF)

1.5.3 *die mandatstragenden Verbände und Organisationen*

Freier Deutscher Gewerkschaftsbund (FDGB)
Freie Deutsche Jugend (FDJ)
Demokratischer Frauenbund Deutschlands (DFD)
Kulturbund der DDR (KB)
Vereinigung der gegenseitigen Bauernhilfe (VdgB)
Konsumgenossenschaft der DDR (KG)

1.5.4 *Verbände und Organisationen ohne Fraktionen in den Volksvertretungen*

Arbeiter- und Bauerninspektion (ABI), einschließlich der Volkskontrollausschüsse
Betriebsakademien
Blinden-und-Sehschwachen-Verband der DDR (BSV)
Bund der Architekten der DDR (BdA)
Deutsche Arbeiterkonferenz
Deutscher Turn- und Sportbund der DDR (DTSB)
Deutsches Rotes Kreuz der DDR (DRK)
Domowina - Bund der Lausitzer Sorben
Friedensrat der DDR (FR)
Gehörlosen-und-Schwerhörigen-Verband der DDR (GSV)
die Genossenschaften
Gesellschaft für Deutsch-Sowjetische Freundschaft (DSF)
die Jagdgesellschaften und deren Dachorganisation
Kammer der Technik (KDT)
Ökonomisches Archiv
Schriftstellerverband der DDR
Solidaritätskomitee der DDR
URANIA der DDR
Verband Bildender Künstler der DDR (VBK)
Verband der Film- und Fernsehschaffenden der DDR (VFF)
Verband der Journalisten der DDR (VDJ)
Verband der Kleingärtner, Siedler und Kleintierzüchter (VKSK)
Verband der Komponisten und Musikwissenschaftler der DDR
Verband der Theaterschaffenden der DDR (VT)

Vereinigung der Juristen der DDR (VdJ)
Volkssolidarität (VS)
die Wissenschaftlichen Gesellschaften

1.5.5 *die paramilitärischen Verbände der DDR*
Gesellschaft für Sport und Technik (GST)
Kampfgruppen der Arbeiterklasse

1.6 Unter dem Begriff des Verarbeitens *für Zwecke der "öffentlichen Verwaltung*" ist jede Tätigkeit anzusehen, die von der vollziehenden Gewalt (der Regierung, den Ministerien und den diesen nachgeordneten Behörden oder sonstigen Dienststellen, den Gemeinden und Landkreisen sowie sonstigen juristischen Personen des öffentlichen Rechts) ausgeübt wurde, ungeachtet ob sie der Eingriffsverwaltung (Eingriff in die Rechts- und Freiheitssphäre des einzelnen) oder der Leistungsverwaltung (der Daseinsvorsorge dienendes Handeln) zuzuordnen ist. Wegen der Unterordnung des Staatsapparates, der Blockparteien sowie der Verbände und Organisationen unter die Beschlüsse und Weisungen des Politbüros der SED ist unter den Begriff des Verarbeitens für Zwecke der "öffentlichen Verwaltung" nicht nur die vorangehend beschriebene Tätigkeit öffentlicher Stellen zu subsumieren, sondern auch *jede Tätigkeit, die auf Machtausübung seitens politischer oder staatlicher Organe der DDR beruhte und die zur Folge hatte, daß das Individuum in ein Abhängigkeitsverhältnis gegenüber der tätigwerdenden Organisation gebracht worden ist.*

1.7 Das Innehaben der *tatsächlichen Gewalt* über die personenbezogenen Daten bedeutet, daß den mittelbaren oder unmittelbaren Besitzer der Daten (Person oder Stelle) ohne Rücksicht darauf, aus welchem Rechtsgrund oder auf Grund welcher tatsächlicher Umstände er in den Besitz gelangt ist, die Meldepflicht trifft. Zur Meldung sind auch die Behörden und sonstigen öffentlichen Stellen des Freistaates
Sachsen, die Gemeinden und Landkreise sowie der sonstigen der Aufsicht des Freistaates unterstehenden juristischen Personen des öffentlichen Rechts verpflichtet.

1.8 *Meldepflichtig* bei Organisationen mit Nebenstellen, Zweigstellen etc. *ist im Zweifel die ausgelagerte Stelle,* insbesondere soweit es sich um Organisationen mit Hauptsitz außerhalb des Freistaates Sachsen handelt.

1.9 *Maßgebender Zeitpunkt* ist für das Innehaben der Altdatenbestände der *14. Dezember 1991* (§ 36 SächsDSG) oder später. Meldepflichtig sind die Personen und Stellen, die an diesem Tag oder danach die tatsächliche Gewalt über die personenbezogenen Daten, die *vor dem 3. Oktober 1990* erhoben oder in anderer Weise verarbeitet worden sind, innehatten oder noch innehaben.

1.10. Nach § 35 Abs. 2 Satz 1 SächsDSG ist über die Akten oder Dateien ein *Verzeichnis* in sinngemäßer Anwendung des § 10 SächsDSG aufzustellen. In dem Verzeichnis sind schriftlich festzuhalten:

1. die Bezeichnung der Akten (Aktensammlung) / Datei und ihre Zweckbestimmung; Auftraggeber / Veranlasser,
2. die Aufgabe, zu deren Erfüllung die Akte (Aktensammlung) / Datei verarbeitet wurde und die Rechtgrundlage bzw. der Grund der Verarbeitung; Zeitpunkt der Beendigung der Auftragsverarbeitung,
3. die Art der gespeicherten Daten (z. B. Personalien, wie Name, Vorname, personengebundene Hinweise),
4. der Kreis der Betroffenen (=bestimmte oder bestimmbare natürliche Personen, über deren persönliche oder sachliche Verhältnisse Einzelangaben gemacht werden),
5. die Art der regelmäßig an Dritte übermittelten Daten und deren Empfänger sowie die Art und Herkunft der regelmäßig empfangenen Daten,
6. entfällt,
7. die früher und heute zugriffsberechtigten Personen oder Personengruppen,
8. die gegenwärtigen personellen, technischen und organisatorischen Maßnahmen (§ 9 SächsDSG) zur Sicherung des Datenbestandes (z. B. Verwahrung in gesondertem Raum / Behältnis, Zugangsberechtigte),
9. (nur bei automatisierten Verfahren) die Betriebsart des Verfahrens, die Art der Geräte sowie die Verfahren zur Übermittlung und Auskunftserteilung,
10. Typ, Art, Hersteller und Gerätenummer der bei der automatisierten Datenverarbeitung eingesetzten Geräte, das verwendete Betriebssystem sowie die Möglichkeiten zur Datenfernverarbeitung und Datenübertragung.
11. Zusätzlich sollte angegeben werden, wer als *Rechtsnachfolger* der öffentlichen Stelle im Sinne des § 35 Abs. 1 SächsDSG anzusehen ist, falls diese nicht mehr besteht. Gegebenenfalls ist dies mit den zuständigen Behörden des Freistaates Sachsen oder der Treuhandanstalt abzustimmen. Dabei sollte auch über den Verbleib der nicht personenbezogenen Daten verhandelt werden.

1.11 Das Verzeichnis ist dem *Sächsischen Datenschutzbeauftragten*, Devrientstraße/Ecke Marienbrücke, 8010 Dresden, *bis zum 31. März 1992 zur Auswertung zuzuleiten. Dabei ist darzulegen, welche Akten, Dateien und Geräte zur rechtmäßigen Aufgabenerfüllung noch erforderlich sind.*

1.12 *Die Akten und Dateien sind* von den Meldepflichtigen unverzüglich *unter Verschluß zu nehmen.*

2. *Hinweis über nicht mehr vorhandene Altdatenbestände*

Nach § 35 Abs. 3 SächsDSG ist *jedermann verpflichtet*, sich an den Sächsischen Datenschutzbeauftragten zu wenden und über nicht mehr vorhandene Akten und Dateien die in § 10 SächsDSG vorgeschriebenen Angaben zu machen (vgl. Nr. 1.10), soweit dies den Umständen und seiner Kenntnis nach noch möglich ist. Dies

gilt insbesondere auch für die meldepflichtigen öffentlichen Stellen im Sinne des Sächsischen Datenschutzgesetzes (vgl. Nr. 1.5), soweit Akten und Dateien ausgelagert, vernichtet oder sonstwie aus ihrem Besitz gelangt sind.

3. *Entscheidung über das Verbleiben der gemeldeten Altdatenbestände*

Das Sächsische Staatsministerium des Innern oder eine von diesem genannte Behörde wird gemäß § 35 Abs. 4 SächsDSG entscheiden,ob und wem die Akten und Dateien sowie die zu ihrer Ordnung, Auffindung oder Auswertung dienenden Materialien und Träger sowie sonstiges Zubehör im Original und sämtlichen Ausfertigungen zu übergeben sind. Dem kann eine Einsichtnahme durch das Sächsische Staatsministerium des Innern, durch eine von diesem genannte Behörde oder durch den Sächsischen Datenschutzbeauftragten vorangehen. Kopien der Altdatenbestände dürfen weder angefertigt noch behalten werden.

4. *Strafbewehrung*

Nach § 35 Abs. 5 SächsDSG wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wer
1. Altdatenbestände, im Sinne des § 35 Abs. 1 oder 3 SächsDSG verheimlicht,
2. die Vorlage eines Verzeichnisses nach § 35 Abs. 2 SächsDSG unterläßt,
3. Akten oder Dateien entgegen § 35 Abs. 4 SächsDSG nicht vorlegt, nicht übergibt oder Kopien anfertigt oder zurückbehält.

5. *Vordruck*

Für die Mitteilung der Verzeichnisse (vgl. Nr. 1) *soll nach Möglichkeit* der nachstehende *Vordruck* verwendet werden, wobei es sich empfiehlt, *einen* Vordruck je Akte (Aktensammlung) /Datei zu benutzen. Der Vordruck ist auch für Hinweise über nicht mehr vorhandene Altdatenbestände (vgl. Nr. 2) mit entsprechenden Änderungen verwendbar.

Giesen

16.1.2 **(SächsABl. S.1295)**

Hinweise des Sächsischen Datenschutzbeauftragten zu den Aufgaben eines internen Datenschutzbeauftragten öffentlicher Stellen (behördlicher Datenschutzbeauftragter) vom 21. August 1992

Das Sächsische Datenschutzgesetz sieht für öffentliche Stellen (§ 2 Abs. 1 SächsDSG) nicht ausdrücklich die Pflicht zur Bestellung eines internen Datenschutzbeauftragten vor. Denn eine gesetzlich vorgeschriebene Institution "interner Datenschutzbeauftragter" könnte dazu führen, daß der Behördenleiter sich von der eigenen Verantwortung für die Einhaltung der datenschutzrechtlichen Vorschriften freigestellt fühlt. Die Leitungsverantwortung verbleibt aber auch hinsichtlich der Beachtung des Rechts auf informationelle Selbstbestimmung stets beim Behördenleiter. Dabei kommt der Ressortverantwortlichkeit der Minister (Art. 63 Abs. 2 der Verfassung des Freistaates Sachsen) sowie der Organisationshoheit als Teil der Selbstverwaltung der Gemeinden, ihrer Verbände und der übrigen Selbstverwaltungsträger (Art. 82 Abs. 2 der Verfassung des Freistaates Sachsen) besondere Bedeutung zu.

Unbeschadet dieser Eigenverantwortlichkeit sollten in größeren Behörden und in Behörden mit Aufgabenvielfalt, d. h. wenn mehrere öffentliche Stellen im Sinne des Datenschutzgesetzes in einer Behörde "gebündelt" sind, interne Datenschutzbeauftragte bestellt werden.

Für den Bereich der von § 35 Sozialgesetzbuch I erfaßten Leistungsträger müssen nach § 79 SGB X interne Datenschutzbeauftragte bestellt werden, wenn dort mindestens fünf Mitarbeiter personenbezogene Daten automatisiert verarbeiten. Die nach § 18 Abs. 2 Bundesdatenschutz-gesetz verlangten Angaben sind nur bezüglich der Sozialdateien dem Sächsischen Datenschutz-beauftragten ohne weitere Aufforderung vorzulegen.

1. Aufgaben

Die Aufgaben des internen Datenschutzbeauftragten orientieren sich im wesentlichen an der Funktion seiner Behörde:

- Er setzt die in § 9 SächsDSG genannten Maßnahmen zum Persönlichkeitsschutz von Bürgern und Mitarbeitern in konkrete Vorschläge um und sichert die Zweckbestimmung der Daten,
- er beteiligt sich an Organisationsentscheidungen zur Zusammenarbeit, Beteiligung oder Abschottung einzelner Stellen innerhalb der Behörde und der Beteiligung fremder Stellen,
- er unterrichtet Personen, die mit der Verarbeitung personenbezogener Daten in Akten oder Dateien betraut sind, über die Grundsätze und praktischen Erfordernisse des Datenschutzes,
- er führt die Dateien- und Geräteverzeichnisse nach § 10 SächsDSG,
- er verpflichtet Mitarbeiter auf das Datengeheimnis nach § 6 Abs. 3 SächsDSG

(Zusammenarbeit mit der Personalverwaltung),
- er gibt Hinweise zur Führung von Akten, zur Entwicklung von Formularen, zur Entwicklung und zum Einsatz von Softwareprogrammen,
- er wirkt bei der Auftragserteilung zur Datenverarbeitung und deren Kontrolle mit (§§ 7 und 9 Abs. 2 SächsDSG),
- er berät den Dienststellenleiter, die Bediensteten und den Personalrat der Dienststelle in allen Fragen des Persönlichkeitsschutzes und einer datenschutzgerechten internen Organisation,
- er kontrolliert, ob Datenschutzvorschriften und hausinterne Datenschutzrichtlinien eingehalten werden und prüft dabei Schwachstellen und Risiken bei der Datensicherheit,
- er berät bei der Vernichtung von Akten sowie der Löschung von Dateien und überprüft den Vernichtungsvorgang.

Weitere Aufgaben können dem internen Datenschutzbeauftragten von seinen Vorgesetzten übertragen werden.

2. Organisatorische Stellung
Der interne Datenschutzbeauftragte muß seine Aufgaben neutral versehen können; an fachliche Weisungen des Vorgesetzten, insbesondere des Dienststellenleiters, bleibt er jedoch gebunden. Die Fachbereiche sollen ihn in seinen Aufgaben unterstützen.

Für die Behördenleitung, die Bediensteten, den Personalrat, Bürger und andere Behörden kommt ihm insgesamt eine koordinierende und beratende Funktion zu. Im Hinblick auf unvermeidliche Interessenkonflikte dürfen ihm berufliche Nachteile weder drohen noch entstehen.

Es ist zulässig, einen Bediensteten (z. B. der Personalverwaltung, des Organisationswesens oder der Datenverarbeitung) neben seiner Hauptaufgabe als internen Datenschutzbeauftragten zu bestellen. Dabei sind jedoch Spannungsverhältnisse zwischen beiden Aufgaben zu vermeiden oder - wenn vorhanden - offen zu klären.

Dem internen Datenschutzbeauftragten sollen schriftlich bestimmte Kontrollbefugnisse verliehen werden (z. B. durch Hausverfügung). Insbesondere soll ihm gewährt werden:

- Auskunft auf Fragen, deren Beantwortung für den internen Datenschutzbeauftragten erforderlich ist,
- Einsicht in Akten, Dateien und sonstige Unterlagen, wenn im Einzelfall oder aus grundsätzlichen Erwägungen Probleme des Persönlichkeitsschutzes zu klären sind (§ 12 Abs. 3 SächsDSG),
- das Recht, Stellungnahmen innnerhalb der Dienststelle einzuholen,
- die Möglichkeit, dem Behördenleiter direkt vorzutragen.

3. Persönliche Eignung
Der interne Datenschutzbeauftragte muß zuverlässig und fachkundig sein. Sofern er über die fachlichen Qualifikationen (verfassungsrechtliche und organisatorische Kenntnisse, Sicherheit im Umgang mit den einschlägigen Spezialvorschriften zum Persönlichkeitsschutz im eigenen Fachbereich und dem Sächsischen Datenschutzgesetz, Grundkenntnisse in automatisierter Datenverarbeitung) noch nicht verfügt, soll ihm Gelegenheit gegeben werden, diese zu erwerben.

4. Vermeidung unnötiger Bürokratie
Richtig verstandener Persönlichkeitsschutz hält die Verwaltung klein und effektiv; Datenschutz gewährleistet, daß nur die zur gesetzlichen Aufgabenerfüllung wirklich erforderlichen Daten erhoben, verarbeitet und übermittelt werden.

Jeder Dienststellenleiter soll den Datenschutz als Führungsinstrument einsetzen: Die Arbeitsvorgänge werden wegen der strikten Zweckbindung aller personenbezogenen Informationen durchschaubar, die Verantwortung wird personalisiert und Kompetenz nach unten verlagert.

Die Organisation des internen Datenschutzes darf keine neuen Verwaltungsstrukturen entstehen lassen, die sinnvolle Verwaltungsabläufe auf klarer gesetzlicher Grundlage behindern oder gar bürokratisieren.

Interner Datenschutz kann nur dann effizient sein, wenn allen Bediensteten das Anliegen des Schutzes der Persönlichkeit durch einfache und verständliche, auf den einzelnen Arbeitsplatz zugeschnittene Hilfestellung vermittelt wird. Nicht erreicht wird dies durch abstrakt und formelhaft umschriebene Zielvorstellungen, die als Hausverfügungen in Umlauf gegeben und - dies zeigt die Praxis - selten von den Mitarbeitern nachvollzogen und umgesetzt werden können.

Datenschutz darf sich nie zum Selbstzweck entwickeln.

Nur durch eigene Kenntnis der individuellen Arbeitsabläufe wird der interne Datenschutz-beauftragte in der Lage sein, bei den Bediensteten die erforderliche Sensibilität im Umgang mit personenbezogenen Daten zu wecken.

Es ist Aufgabe des internen Datenschutzbeauftragten, das Grundrecht auf Schutz der Privatsphäre nicht durch Bürokratie, sondern durch eigenverantwortliches Handeln aller Bediensteten zu sichern.

Dresden, den 21. August 1992

Der Sächsische Datenschutzbeauftragte
Thomas Giesen

16.1.3 **SächsABl. 1993 S.50**

Bekanntmachung des Sächsischen Datenschutzbeauftragten zu § 31 Abs. 7 des Sächsischen Datenschutzgesetzes (SächsDSG) vom 10. Dezember 1992

Nach § 31 Abs. 7 SächsDSG darf eine *automatisierte Verarbeitung von Personaldaten* durch öffentliche Stellen in Sachsen *nur im Benehmen mit dem Sächsischen Datenschutzbeauftragten* eingeführt, angewendet, geändert oder erweitert werden.
Diese Bestimmung wird in der behördlichen Praxis weitgehend nicht beachtet. So werden z. B. Telekommunikationsanlagen und Zeiterfassungsgeräte ohne vorherige Information des Datenschutzbeauftragten installiert. Ohne die vorgeschriebene Beteiligung ist es dem Datenschutzbeauftragten nicht möglich, seinem Beratungs- und Kontrollauftrag gemäß § 24 SächsDSG aus-reichend nachzukommen. Seine Beurteilung der automatisierten Personaldatenverarbeitung ist auch für die Entscheidung der *Personalvertretung* von Bedeutung.
Um dem Datenschutzbeauftragten einen Überblick über die bereits eingesetzten Verfahren zur Personaldatenverarbeitung und die Beurteilung zu ermöglichen, ob ein Verfahren den Grund-sätzen der Rechtmäßigkeit und Erforderlichkeit entspricht, werden alle öffentlichen Stellen (§ 2 SächsDSG) aufgefordert, zu noch nicht gemeldeten Verfahren folgende Angaben zu machen und gegebenenfalls durch entsprechende Unterlagen zu ergänzen:

1. Beschreibung des Verfahrens mit Angabe des betroffenen Personenkreises
2. Art des EDV-Verfahrens (z. B. Online- oder Batch-Betrieb)
3. Beschreibung des speicherungsfähigen Datensatzes bis auf Feldebene mit Angabe der Rechtsgrundlage für die Speicherung bzw. Verarbeitung
4. Datenübermittlungen mit Angabe der Rechtsgrundlage(n)
   4.1 Beschreibung des jeweiligen Übermittlungsdatensatzes bis auf Feldebene
   4.2 Art der Datenübermittlung
   4.3 Datenempfänger
   4.4 Turnus der Datenübermittlung
5. Stelle, die für die Systementwicklung und Programmierung des Verfahrens zuständig ist
6. Rechenzentrum oder Stelle der Datenverarbeitung
7. Vertrag mit dem Auftragnehmer bei Datenverarbeitung im Auftrag nach § 7 SächsDSG
8. Dienstvereinbarung mit dem Personalrat / Sonstige Beteiligung der Personalvertretung

Die gesetzlich ausdrücklich bestimmte Beteiligung des Sächsischen Datenschutzbeauftragten soll nicht zu unangemessener Entscheidungsverzögerung führen. Deshalb ist seine frühzeitige und umfassende Information anzuraten.
In vielen Fällen kann mit einer umgehenden Empfehlung gerechnet werden.

Merkblatt des Sächsischen Datenschutzbeauftragten zum Betrieb digitaler Telekommunikationsanlagen vom 8. Januar 1993

1. Datenspeicherung

In digitalen Telekommunikationsanlagen (TK-Anlagen) werden folgende personenbezogene Daten gespeichert und ggf. verarbeitet:

- *Anschlußdaten*

Für jede Nebenstelle (Endstelle, Anschluß) werden administrative Anschlußdaten gespeichert: Name des Anschlußinhabers, Leistungsmerkmale (Amtsberechtigung, Aufschalten etc.), Kurzwahlziele (häufig verwendete Telefonnummern), Geheimcode zur Sperrung des Endgerätes sowie die zuletzt gewählte Verbindung. Die Generierung der Nebenstelle und die Eingabe der Leistungsmerkmale von einem Systemverwalter, der auch für die Pflege der Daten zuständig ist, werden an einem sog. Betriebsterminal vorgenommen.

- *Verbindungsdaten* (Gesprächsdaten)

Für jede abgehende Verbindung wird meist ein Datensatz gespeichert, der neben der Rufnummer des Anrufers und des Angerufenen Angaben über Zeitpunkt, Dauer und Art der Verbindung (Telefon, Telefax usw.) enthält. Diese Daten werden bei Bedarf (in der Regel monatlich) im sog. Gebührencomputer ausgewertet. Jeder Hersteller bietet Programme an, die eine vielseitige Auswertung dieser Verbindungsdaten gestatten. So können beispielsweise zur Abrechnung geführter Privatgespräche monatlich Listen erstellt werden. Darüber hinaus können die Verbindungsdaten auch zur Kontrolle benutzt werden (Auflistung der teuersten und häufigsten Gespräche, Häufigkeitsstatistik über die Anzahl der Gespräche je Anschluß).

2. Zulässigkeit der Datenspeicherung

Die Verarbeitung personenbezogener Daten in TK-Anlagen durch sächsische Behörden unterliegt den Zulässigkeitsvoraussetzungen des Sächsischen Datenschutzgesetzes (vor allem dem "Erforderlichkeitsgrundsatz") und hat die Sicherheitsanforderungen des Gesetzes zu erfüllen. Darüber hinaus sind jedoch wesentlich die Vorschriften zu beachten, die das Verhältnis zwischen Bediensteten und Dienstherrn regeln, wie zum Beispiel das Bundespersonalvertretungsgesetz bzw. sächsisches Personalvertretungsrecht (insbesondere wären dies einschlägige Vereinbarungen zwischen Dienstherrn und Bediensteten, in der Regel in Form von Dienstvereinbarungen). Aus Sicht des Datenschutzes können nur solche Datenverarbeitungen als erforderlich und somit zulässig angesehen werden, die

durch entsprechende Vorschriften gedeckt sind. Weitergehende Verarbeitungen können nur mit Einwilligung der Betroffenen erfolgen.

3. Mitbestimmungs- bzw. Mitwirkungsrecht

Die Verbindungsdaten, die in einer TK-Anlage gespeichert werden, sind geeignet, für eine Verhaltens- oder Leistungskontrolle der Bediensteten verwendet zu werden (vgl. die Entscheidung des Bundesverwaltungsgerichts vom 16.12.1987, Nr. 6 - P 32/84). TK-Anlagen mit Gesprächsdatenerfassung sind daher nach § 75 Abs. 3 Nr. 17 des Bundespersonalvertretungsgesetzes bzw. nach einer entsprechenden Bestimmung in einem Sächsischen Personalvertretungsgesetz mitbestimmungspflichtig. Vor der Beschaffung einer TK-Anlage sollte deshalb der Personalrat über die Einzelheiten der geplanten Verarbeitungen und Nutzungen informiert werden. Vor allem sollten die angestrebten Auswertungen dieser Daten in einer Dienstvereinbarung geregelt werden.

4. Dienstliche Telefongespräche

Eine Speicherung und Auswertung aller Verbindungsdaten einschließlich der vollständigen Rufnummer des Angerufenen *der Diensttelefongespräche* ist nur zulässig, wenn diese Daten für eine Kostenkontrolle, im Rahmen einer Fach- oder Dienstaufsicht oder für ein Datenschutzkontrolle benötigt werden. Die Daten dürfen nur für diese Zwecke verwendet und nicht mit anderen automatisierten Personaldateien verknüpft werden. Sie dürfen nur den mit der Kontrolle beauftragten Personen zugänglich gemacht werden und sind nach Abschluß der Kontrolle - spätestens nach einer festzulegenden Frist (etwa nach 1 Jahr) - zu löschen.

5. Private Telefongespräche

Soweit die Führung privater Telefongespräche zugelassen ist, sind diese besonders zu kennzeichnen. Bei *Privatgesprächen* ist die Verbindungsdatenspeicherung nur in dem Umfang zulässig, in dem sie zur Überprüfung der vom Dienstherrn erstellten Telefonrechnung durch den Bediensteten erforderlich und in einer Dienstvereinbarung geregelt ist. Diese Daten dürfen nur für Abrechnungszwecke verwendet werden. Beim Ausdruck der Daten von Privatgesprächen ist die angewählte Rufnummer (verkürzte Zielnummerspeicherung ohne die beiden letzten Ziffern) zu unterdrücken. Nach der Bezahlung der vom Dienstherrn gestellten Telefonrechnung sind die Daten über geführte Privatgespräche zu löschen.

Die Bediensteten sollten in einer Dienstanweisung darauf hingewiesen werden, daß beim Führen von privaten Ferngesprächen bestimmte Gesprächsdaten (Art der Daten) gespeichert, teilweise ausgedruckt und für die Abrechnungszwecke verwendet werden.

6. Datensicherheit

Die gespeicherten personenbezogenen Daten - insbesondere die Gesprächsdaten - sind gegen unbefugte Einsichtnahme und Veränderung technisch und organisatorisch zu sichern. Das Betriebsterminal der TK-Anlage darf *nur* dem Systemverwalter zugänglich sein (abgeschotteter Bereich).

Die Berechtigung, Daten einzugeben, zu löschen oder zu verändern, ist auf den Systemverwalter und seinen Vertreter zu begrenzen und durch ein persönliches Kennwort (Paßwort) abzusichern. Für den Vertretungsfall sollte das Paßwort in einem versiegelten Umschlag bereitgestellt werden. Das Paßwort ist regelmäßig zu ändern und muß mindestens 6 Stellen lang sein. Trivialpaßwörter sind zu vermeiden.

7. Wartung, Fernwartung

Fernwartung durch den Hersteller sollte nur dann zugelassen werden, wenn sichergestellt ist, daß

a) ein Zugriff durch das Fernwartungszentrum auf die TK-Anlage auch im Einzelfall nur unter Mitwirkung des Systemverwalters (z.B. durch Betätigen eines Schalters, Freigabe am Betriebsterminal) möglich ist und
b) bei einem solchen Zugriff keine Möglichkeit besteht, personenbezogene Daten einzusehen, zu ändern oder zu kopieren.

Der Hersteller sollte die Wartungsaktivitäten schriftlich dokumentieren und den Nichtzugriff auf personenbezogene Daten vertraglich bestätigen.

Programme, bei denen der Zugriff auf personenbezogene Daten unerläßlich ist, dürfen nur am Betriebsterminal und ebenfalls unter Mitwirkung des Systemverwalters zu starten sein. Solche Fälle sollten aber den Ausnahmefall darstellen.

Die Wartung hat sich durch ein entsprechendes Paßwort, das nicht mit der Systemverwalterkennung identisch ist, zu identifizieren. In solchen Fällen haben sich Doppelpaßwortverfahren bewährt. Im übrigen ist über die Wartungsarbeiten ein Logbuch zu führen.

8. Dokumentation

Der Systemverwalter muß eine Übersicht führen, aus der hervorgeht, welche Nebenstelle über welche Leistungsmerkmale verfügt. Bei dieser Übersicht ist auf die Revisionsfähigkeit zu achten.

9. Dateien- und Geräteverzeichnis

Eine Gesamtübersicht über die Konfiguration der TK-Anlage ist zu führen.
§ 10 SächsDSG ist zu beachten.

10. Beteiligung des Sächsischen Datenschutzbeauftragten

Nach § 31 Abs. 7 SächsDSG darf eine automatisierte Verarbeitung von Personaldaten nur um Benehmen mit dem Datenschutzbeauftragten eingeführt, angewendet, geändert oder erweitert werden. Dies gilt auch für TK-Anlagen.

Dresden, 8. Januar 1993
Der Sächsische Datenschutzbeauftragte
Thomas Giesen

16.2 Entschließungen der Datenschutzbeauftragten des Bundes und der Länder

16.2.1 Entschließung der 43. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 23./24. März 1992 in Stuttgart zum Arbeitnehmerdatenschutz

I. Im Rahmen des Arbeitsverhältnisses werden personenbezogene Daten aus ganz unterschiedlichen Lebensbereichen des Arbeitnehmers erhoben und gespeichert. Diese Daten verwendet der Arbeitgeber nicht nur für eigene Zwecke. Aus dem Arbeitsverhältnis ergeben sich auch Auskunfts-, Bescheinigungs- und Meldepflichten, die der Arbeitgeber gegenüber öffentlichen Stellen zu erfüllen hat. Durch die Möglichkeit, im Arbeitsverhältnis anfallende personenbezogene Daten miteinander zu verknüpfen und sie - losgelöst vom Erhebungszweck -für andere Verwendungen zu nutzen, entstehen Gefahren für das Persönlichkeitsrecht des Arbeitnehmers. Mit der Intensität der Datenverarbeitung, insbesondere durch Personalinformationssysteme und digitale Telekommunikationsanlagen, nehmen die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebers zu.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb bereits seit 1984 bereichsspezifische und präzise gesetzliche Bestimmungen zum Arbeitnehmerdatenschutz. Bundestag, Bundesrat und Bundesregierung haben ebenfalls eine Regelungsnotwendigkeit bejaht; gleichwohl stehen bundesgesetzliche Regelungen über den allgemeinen Arbeitnehmerdatenschutz immer noch aus.

Die Notwendigkeit zur gesetzlichen Regelung besteht unabhängig davon, ob Arbeitnehmerdaten in automatisierten Dateien, in Akten oder in sonstigen Unterlagen verarbeitet werden. Der erhöhten Gefährdung durch die automatisierte Datenverarbeitung ist durch spezifische Schutzvorschriften Rechnung zu tragen.

Angesichts der besonderen Abhängigkeit des Arbeitnehmers im Arbeitsverhältnis und während der Phase einer Bewerbung um einen Arbeitsplatz ist durch Gesetz zu untersagen, daß Rechte, die dem Arbeitnehmer nach einschlägigen Datenschutzvorschriften zustehen, durch Rechtsgeschäft, Tarifvertrag und Dienst- oder Betriebsvereinbarung ausgeschlossen werden. Außerdem ist durch Gesetz festzulegen, daß eine Einwilligung des Arbeitnehmers oder Bewerbers nur dann als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung in Frage kommt, wenn die Freiwilligkeit der Einwilligung sichergestellt ist, also die Einwilligung ohne Furcht vor Nachteilen verweigert werden kann. Deshalb dürfen allein aufgrund einer Einwilligung z. B. keine Gesundheitszeugnisse, Ergebnisse von Genomanalysen u. ä. angefordert werden, wenn sie den Rahmen des Fragerechts des Arbeitgebers überschreiten.

II. Die gesetzliche Ausgestaltung des Arbeitnehmerdatenschutzes muß insbesondere folgende Grundsätze beachten:

1 . Die Datenerhebung muß grundsätzlich beim Arbeitnehmer erfolgen.

2. Der Arbeitgeber darf Daten des Arbeitnehmers - auch durch Befragen des Arbeitnehmers oder Bewerbers - nur erheben, verarbeiten oder nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgesehen ist. Dabei ist der Grundsatz der Zweckbindung zu beachten. Auch ist zwischen der Bewerbungs- und Einstellungsphase zu unterscheiden.
3. Der Arbeitgeber darf Daten, die er aufgrund gesetzlicher Vorgaben für andere Stellen (z. B. Sozialversicherungsträger) erheben muß, nur für diesen Zweck verwenden.
4. Eine Datenauswertung und -verknüpfung, die zu Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers führen kann, ist unzulässig.
5. Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.
6. Notwendige Datenübermittlungen zwischen Arzt und Arbeitgeber sind eindeutig zu regeln. Dem Arbeitgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung zugänglich gemacht werden. Darüber hinaus dürfen ihm - soweit erforderlich - nur tätigkeitsbezogene Risikofaktoren mitgeteilt werden. Medizinische und psychologische Befunde sind getrennt von den übrigen Personalunterlagen aufzubewahren. Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests des Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz des Beschäftigten dient.
7. Dem Arbeitnehmer sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die sein Arbeitsverhältnis betreffen. Diese Rechte müssen sich auch auf Herkunft, Verarbeitungszwecke und Empfänger der Daten sowie die Art und Weise ihrer Auswertung erstrecken.
8. Dem Personal-/Betriebsrat muß ein Mitbestimmungsrecht bei der Einführung, Anwendung und der wesentlichen Änderung von automatisierten Dateien mit personenbezogenen Daten der Arbeitnehmer für Zwecke der Personalverwaltung zustehen. Das gilt auch bei sonstigen technischen Einrichtungen, mit denen das Verhalten und die Leistung der Beschäftigten überwacht werden kann.
9. Gesetzlich festzulegen ist, welche Daten der Arbeitnehmervertretung für ihre Aufgabenerfüllung zugänglich sein müssen und wie der Datenschutz bei der Verarbeitung von Arbeitnehmerdaten im Bereich der Arbeitnehmervertretung gewährleistet wird. Regelungsbedürftig ist auch das Verhältnis zwischen dem Personal-/Betriebsrat und dem behördlichen/betrieblichen Datenschutzbeauftragten.

10. Die Befugnis des Personal-/Betriebsrats, sich unmittelbar an die Datenschutzkontrollinstanzen zu wenden, ist gesetzlich klarzustellen.

11. Arbeitnehmerdaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist oder wenn der Betroffene nach den oben genannten Grundsätzen (vgl. Abschn. 1 Abs. 4) eingewilligt hat.

16.2.2 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Grundrecht auf Datenschutz vom 28. April 1992

1. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 ist allgemein anerkannt, daß die Grundrechte auch die Befugnis des einzelnen umfassen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Die Datenschutzbeauftragten treten dafür ein, dieses Recht ausdrücklich im Grundgesetz zu verankern. Damit würde

- für die Bürger deutlicher erkennbar, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte,
- der wachsenden Bedeutung des Datenschutzes für das Funktionieren der freiheitlichen Demokratie
- Rechnung getragen und auf die negativen Erfahrungen der DDR-Geschichte reagiert,
  der Grundrechtskatalog dem technologischen Wandel angepaßt und
- die Konsequenz aus den positiven Erfahrungen gezogen, die in mehreren Ländern des Bundes und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.

Die Konferenz begrüßt deshalb die Vorstellungen, die in der Verfassungskommission des Bundesrates entwickelt worden sind.

Die Datenschutzbeauftragten empfehlen der Gemeinsamen Verfassungskommission des Bundestages und Bundesrates im Zusammenhang mit Art. 1 und Art. 2 GG den nachfolgenden Text zur Beratung:

> *»Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Dazu gehört das Recht aufAuskunft und Einsicht in amtliche Unterlagen. Dieses Recht darf nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern. «*

2. Darüber hinaus empfiehlt die Konferenz, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.

3. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es zusätzlich für erforderlich, in die Verfassungsdiskussion folgende Punkte miteinzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:
   - Stärkung der Grundrechte aus Art. 10 und 13 im Hinblick auf neue Überwachungstechniken
   - Recht auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit)
   - Instrumente zur Technikfolgenabschätzung

16.2.3 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Neuregelung des Asylverfahrens (BT-Drs. 12/2062) vom 28. April 1992

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält Änderungen des Gesetzentwurfs zur Neuregelung des Asylverfahrens für erforderlich, insbesondere der geplanten Regelungen

1. über die erkennungsdienstliche Behandlung von Asylbewerbern zur Sicherung der Identität (§ 16 Abs. 1) und

2. über die Nutzung der dabei gewonnenen erkennungsdienstlichen Unterlagen zur Strafverfolgung und zur Gefahrenabwehr (§ 16 Abs. 5).

zu 1.

Nach dem geltenden Recht sind Lichtbilder und Fingerabdrücke bei Asylbewerbern nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt ist. Demgegenüber sieht der Gesetzentwurf zur Neuregelung des Asylverfahrens vor, daß von sämtlichen Asylbewerbern - bis auf wenige Ausnahmen - Lichtbilder und Fingerabdrücke zu fertigen sind. Dies ist mit dem Verfassungsgrundsatz der Verhältnismäßigkeit nicht vereinbar:

Der Staat hat selbstverständlich das Recht zu wissen, mit wem er es zu tun hat. Jeder gleichgültig ob Deutscher oder Ausländer - muß sich deshalb durch Dokumente ausweisen können; nur wenn Zweifel an der Identität bestehen, kommen erkennungsdienstliche Maßnahmen in Betracht. Dieser Grundsatz unserer Rechtsordnung muß auch im Rahmen der Neuregelung des Asylverfahrens beachtet werden. Nur wenn feststeht, daß die Identität eines hohen Anteils der Asylbewerber - also nicht bloß diejenige einzelner oder bestimmter Gruppen -zweifelhaft ist, wäre eine erkennungsdienstliche Behandlung aller Asylbewerber gerechtfertigt. Gerade dies aber ist bisher nicht hinreichend belegt: In der amtlichen Begründung des Gesetzentwurfs ist allein davon die Rede, daß nach Feststellung niederländischer Behörden 20 % der Asylbewerber unter falschem Namen einen weiteren Asylantrag stellen. Aussagekräftige Angaben, in welchem Umfang in der Bundesrepublik Deutschland Asylbewerber unter Täuschung über ihre Identität gleich bei der ersten Antragstellung

oder nach dessen Ablehnung erneut versuchen, Asyl zu erhalten, fehlen bislang.

Zu 2.:

Bei der zentralen Auswertung der Fingerabdrücke von Asylbewerbern durch das Bundeskriminalamt muß - ungeachtet dessen, ob das Bundeskriminalamt dabei in eigener Zuständigkeit oder für das Bundesamt für die Anerkennung ausländischer Flüchtlinge tätig wird -unbedingt folgendes sichergestellt sein:

- Fingerabdrücke von Asylbewerbern, die unter Beachtung des zu Nr. 1 Gesagten gefertigt wurden, dürfen nur gespeichert werden, soweit dies zur Sicherung der Identität unbedingt erforderlich ist. Dazu reicht die bisher vom Bundeskriminalamt angewandte Methode der sog. Kurzsatzverformelung der Fingerabdrücke aus. Gerade aber dabei soll es nicht bleiben: Mit der bevorstehenden Einführung von AFIS - einem neuen automatisierten Fingerabdruckverfahren - sollen künftig auch die Fingerabdrücke von Asylbewerbern, die allein zur Feststellung deren Identität gefertigt wurden, genauso erfaßt und ausgewertet werden wie die Fingerabdrücke mutmaßlicher oder tatsächlicher Straftäter. Asylbewerber würden damit von vornherein wie Straftäter behandelt. Eine solche Verfahrensweise wird dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot nicht gerecht. Zudem unterläuft sie die in § 16 Abs. 4 des Gesetzentwurfs vorgesehene Trennung der erkennungsdienstlichen Unterlagen von Asylbewerbern und Straftätern. Um die gebotene Differenzierung sicherzustellen, sollte - über das Trennungsgebot des § 16 Abs. 4 hinaus -die Verformelung auf den Abdruck eines Fingers des Asylbewerbers beschränkt werden, da dies zur eindeutigen Feststellung seiner Identität genügt.

- Die Datenschutzbeauftragten verkennen nicht, daß es unter Umständen im Überwiegenden Allgemeininteresse notwendig sein kann, im Rahmen asylrechtlicher Identitätsfeststellung gefertigte Fingerabdrücke für Zwecke der Strafverfolgung zu nutzen. Weil eine solche Verwendung einen neuen und zudem erheblichen Eingriff in das Grundrecht auf Datenschutz darstellt, darf sie nicht - wie es der Gesetzentwurf aber vorsieht - praktisch voraussetzungslos erfolgen. Notwendig ist vielmehr, die Voraussetzungen in einem abschließenden Straftatenkatalog aufzuführen; darin könnten auch die in der amtlichen Begründung des Gesetzentwurfs erwähnten Fälle des Sozialhilfebetrugs enthalten sein.

- Ein entsprechender Maßstab ist an die Regelung anzulegen, wann zur Identitätssicherung gefertigte Fingerabdrücke von Asylbewerbern zur polizeilichen Gefahrenabwehr genutzt werden dürfen. Eine solche Nutzung sollte nur zugelassen werden, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

16.2.4 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Datenschutz bei internen Telekommunikationsanlagen

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichsspezifische Regelungen entgegengewirkt werden muß. Telefongespräche stehen - auch wenn sie von einem Dienstapparat aus geführt werden - unter dem Schutz des Grundgesetzes. Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben. Der Schutz des Fernmeldegeheimnisses und des nichtöffentlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestitrunungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diesen Anlagen - insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind -umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur Verhaltens- und Leistungskontrolle eignen und zudem Hinweise auf das Kommunikationsverhalten aller Gesprächsteilnehmer geben.

Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TK-Anlagen geben und den Umfang der zulässigen Datenverarbeitung festlegen:

- Es müssen die technischen Voraussetzungen gewährleistet sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.
- Die automatische Speicherung der Rufnummern von externen Anrufem nach Beendigung des Telefongesprächs ist auszuschließen, es sei denn, eine sachliche Notwendigkeit besteht hierfür (z. B. bei Feuerwehr und Rettungsdiensten).
- Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.
- Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollte nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.
- Verbindungsdaten einschließlich der angerufenen Telefonnummern sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.
- Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden.

Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden Mitbestimmungsrechte der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und von wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

16.2.5 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung Gesundheits-Strukturgesetz 1993 - (BR-Drs. 560/92)

Die Bundesregierung will mit dem Gesundheits-Strukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses begrüßenswerte Ziel soll nach dem vorgelegten Gesetzentwurf u. a. auch durch eine verstärkte automatisierte Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die sie schützende ärztliche Schweigepflicht müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hält vor allem folgende Verbesserungen des Gesetzentwurfs für notwendig:

- Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.

- Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.

- Beim Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die Einschaltung privater Abrechnungsstellen ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie - auch zur Abrechnung - im Krankenhaus verbleiben. Die Krankenhäuser sind zudem

selbst in der Lage, die Vergütung einzuziehen.

- Für die neu vorgesehenen Patienten-Erhebungsbogen zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Löschungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbogen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen.

16.2.6 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum »Lauschangriff«

Die Datenschutzbeauftragten des Bundes und der Länder erklären (bei Gegenstimme des LfD Bayern):

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahmen noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heinfliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. »Lauschangriff«) zu ermöglichen.

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein »Innenraum« verbleiben, in dem er »sich selbst besitzt« und »in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt« (BVerfGE 27,1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung - insbesondere heimlicher - entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere nicht das Menschenbild des Grundgesetzes verletzen.

2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitserforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.

3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z. B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs,

Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

16.2.7 Konferenz der Datenschutzbeauftragten des Bundes und der Länder

45. Sitzung, 16./17. Februar 1993, in Berlin Beschluß (zu Protokoll, TOP 4) zum geänderten Vorschlag der EG-Kommission für eine Datenschutzrichtlinie (KOM 92/422 endg.)

Die Konferenz der Datenschutzbeauftragten tritt auf der EG-Datenschutzkonferenz, gegenüber der EG-Kommission sowie den in Deutschland mit der Richtlinie befaßten Ministerien und Gremien (z. B. dem »Düsseldorfer Kreis«) u. a. für folgende Positionen ein:

1. Ein über den durch die Richtlinie harmonisierten Standard hinausgehender Datenschutz im einzelstaatlichen Recht für Datenverarbeitung ohne grenzüberschreitenden Bezug muß zulässig bleiben.

2. Die Meldepflicht zum Dateienregister sollte selektiv ausgestaltet werden. Dem nationalen Gesetzgeber ist dabei mehr Spielraum für die Regelung von Ausnahmefällen einzuräumen.

3. Die Zulässigkeit der Speicherung/Nutzung einerseits und der Übermittlung andererseits ist differenziert zu regeln.

4. Die in der Richtlinie statuierte Unabhängigkeit der nationalen (Datenschutz-) Kontrollbehörden von Regierung und Exekutive muß unangetastet bleiben.

5. In der Richtlinie sollte dem einzelstaatlichen Gesetzgeber ausdrücklich die Option eröffnet werden, eine Kontrollinstitution innerhalb datenverarbeitender Stellen (betrieblicher bzw. behördlicher Beauftragter für den Datenschutz) vorzusehen.

16.3 Sonstiges

16.3.1 Checkliste und Kurzbericht für die Kontrolle öffentlicher Stellen zur Einhaltung des Sächsischen Datenschutzgesetzes (§ 24 Abs. 1 SächsDSG)

Beim Datenschutz stecken die praktischen Probleme immer in den Details eines jeden Falles.
Wie läßt sich da die Einhaltung des Datenschutzes kontrollieren und auf seine Verbesserung Einfluß nehmen?

Als Mittel für die Prüfung haben sich in der Datenverarbeitung und Organisation seit langem Checklisten bewährt. Sie helfen, Prüfungsdetails nicht zu übersehen. Checklisten sind wertvolle Gedächtnisstützen und Gerüst - auch für die Prüfung des Datenschutzes. Ausgefüllte Checklisten fassen das Ergebnis einer Prüfung zusammen und sind damit schon eine Art Kurzbericht über die ausgeführte Prüfung, ohne selbstverständlich einen ausführlichen Bericht ersetzen zu können. Das entspricht meinen ersten Erfahrungen.

Nachfolgend veröffentliche ich Checklisten für eine grobe erste Prüfung hinsichtlich der Einhaltung des Sächsischen Datenschutzgesetzes. Sie können Aufsichtsbehörden und interne Datenschutzbeauftragte anleiten und die interne Datenschutzarbeit erleichtern. Zugleich helfen diese Listen, einen angekündigten Prüfungsbesuch durch den Sächsischen Datenschutzbeauftragten vorzubereiten. Damit soll auch einem Wunsch von behördlichen Datenschutzbeauftragten entsprochen werden.

Es ist vorgesehen, die Checklisten aufgrund weiterer Erfahrungen zu aktualisieren.

Checkliste für Datenschutzkontrollen **Stand: 31.3.93**

Geprüfte öffentliche Stelle
Name:
Anschrift:
Telefon: Fax:

Tag und Ort der Prüfung(en)
Datum: Ort:
1.
2.
3.

Prüfpartner der öffentl. Stelle
Name: Funktion: Telefon:

Prüfer des Sächsischen DSB
Name: Funktion: Telefon:

Kontrollanlaß:
Spezielle Prüfungsziele/ Schwerpunkte der Prüfung

1. kursorische Kontrolle der Einhaltung des SächsDSG:
2.
3.

☐ Bemerkungen zum Ablauf der Kontrolle:

☐ Folgende Unterlagen des Sächs. Datenschutzbeauftragten wurden übergeben (Gesetze, Hinweise, Merkblätter):

1.
2.
3.

Allgemeine Angaben zum Arbeitsprozeß und zum internen Datenschutz

☐ 1.1. Geschäftsverteilungsplan
(als Anlage zu diesem Kontrollbericht)
☐ 1.2. Aktueller Organisationsplan der Datenverarbeitung
(als Anlage zu diesem Kontrollbericht)
☐ 1.3. Übersicht zur Datenverarbeitung (Hardware-, Software-Konfiguration)
(als Anlage zu diesem Kontrollbericht)
☐ 1.4. Spezielle Gesetze und Vorschriften, welche die Aufgaben und Verfahren der öffentlichen Stelle regeln
☐ 1.5. Interner Datenschutzbeauftragter bestellt ?
Name: Funktion: Telefon:
seit (Datum):
☐ 1.6. Schriftlich Kontrollbefugnisse verliehen? (Kopie in die Anlage)
☐ 1.7. Hinweise zu den Aufgaben des internen DSB (Sächs.AmtsBl. Nr.25/1992, S.1295) beachtet?
☐ 1.8. Organisatorische Stellung des internen DSB:
☐ 1.9. Liegen interne Datenschutzregelungen (eigene, übernommene) vor?
(Kopie in die Anlage)
☐ 1.10. Liegt Sicherheitskonzept vor (insgesamt, für welche interne Stelle)?
(Kopie in die Anlage)

Verpflichtung der Personen, die mit der Verarbeitung personenbezogener Daten beschäftigt sind, auf Datengeheimnis (§ 6 SächsDSG)

☐ 2.1. Erfolgte Unterrichtung über die zu beachtenden Vorschriften (wann, durch wen)?
☐ 2.2. Betreffender Personenkreis (welcher) schriftlich auf Datengeheimnis verpflichtet?
(Kopie der Verpflichtungsformulare in die Anlage)
☐ 2.3. Termin der Verpflichtung (31.3.92 nach § 34 Abs.1 u. § 6 Abs.1 SächsDSG) eingehalten am:
☐ 2.4. Wie ist die Aktualisierung der Unterrichtung /Verpflichtung gewährleistet?
☐ 2.5. Wurden alle Personen des Personenkreises verpflichtet?
☐ 2.6. Erfolgte Stichprobenkontrolle in den Personalunterlagen, was ist das Ergebnis?

Anmerkungen:

Dateien -und Geräteverzeichnisse (§ 10 SächsDSG)

- ☐ 3.1. Dateien- und Geräteverzeichnisse liegen vor? (Kopien in die Anlage)
- ☐ 3.2. Angeforderten Dateien und Geräteverzeichnisse wurden übergeben
- ☐ 3.3. Erstellungsdatum der Verzeichnisse (Termin war 31.3.92)
- ☐ 3.4. Wie wird Aktualisierung gesichert ?
- ☐ 3.5. Vollständigkeit der Verzeichnisse?
- ☐ 3.6. Erfolgte Stichprobenkontrolle ?

Anmerkungen:

Automatisiertes Abrufverfahren für personenbezogene Daten (§ 8 SächsDSG)

- ☐ 4.1. Automatisiertes Verfahren (welches) zur Übermittlung von personenbezogenen Daten durch Abruf benutzt?
- ☐ 4.2. Welche gesetzliche Grundlage?
- ☐ 4.3. Automatisiertes Verfahren für den Abruf personenbezogener Daten innerhalb eineröffentlichen Stelle?
- ☐ 4.4. Verfahren angemessen für die Aufgabenerfüllung?
- ☐ 4.5. Stichprobenweise Kontrolle des Abrufs gewährleistet (womit)?
- ☐ 4.6. Wurde das Abrufverfahren schriftlich festgehalten (Anlaß, Zweck, Datenempfänger, abrufbare Daten, Datenschutzmaßnahmen)?
- ☐ 4.7. Wurde der Sächsische Datenschutzbeauftragte informiert? Wenn ja, wann?

Anmerkungen:

Automatisierte Verarbeitung von Beschäftigtendaten (§ 31 Abs. 7 SächsDSG)

- ☐ 5.1. Automatisierte Verarbeitung von Beschäftigendaten eingeführt, angewendet, geändert oder erweitert (Welches Verfahren für welche Beschäftigte)?
- ☐ 5.2. Welche gesetzliche Grundlagen, Rechtsvorschriften oder schriftliche Einwilligungen liegen vor?
- ☐ 5.3. Wurde das Verfahren zur Personaldatenverarbeitung dem Sächs. Datenschutzbeauftragten gemeldet (Bekanntmachung des Sächs.DSB im Sächs. Amtsblatt 1993/Nr. 21, S.30)?
- ☐ 5.4. Wurde die Angaben gemäß Bekanntmachung des Sächs.DSB im Sächs. Amtsblatt 1993/Nr. 21, S.30) gemacht?
- ☐ 5.5. Ins Benehmen gesetzt mit dem Datenschutzbeauftragten und wann?
- ☐ 5.6. Erhielt die zuständige Personalvertretung die Stellungnahme des Datenschutzbeauftragten im Rahmen des Beteiligungsverfahrens (Was ist das Ergebnis)?

Angemessene Maßnahmen zur Gewährleistung des Datenschutzes
(§ 9 SächsDSG)

- ☐ 6.1. Sind besondere Schutzmaßnahmen für die Daten und ihre Verarbeitung erforderlich?
- ☐ 6.2. Wurden unterschiedliche Arten von Schutzbedürftigkeit ("Sensibilität") der Daten erkannt und entsprechend die Arbeit organisiert?
- ☐ 6.3. Welche unterschiedlichen Stufen (Grad) der Schutzbedürftigkeit sind als Grundlage für angemessene Maßnahmen festgelegt (Kopie in die Anlage)?
- ☐ 6.4. Sind diese festgelegten Stufen der Schutzbedürftigkeit angemessen?
- ☐ 6.5. Erfolgte Stichprobenkontrolle und mit welchem Ergebnis?
- ☐ 6.6. Zugangskontrolle
  - ○ personelle Maßnahmen ○ organisatorische Maßnahmen
  - ○ technische Maßnahmen

- ☐ 6.7. Datenträgerkontrolle (auch Aufbewahrung, Löschung, Vernichtung)
  - ○ personelle Maßnahmen ○ organisatorische Maßnahmen
  - ○ technische Maßnahmen

- ☐ 6.8. Speicherkontrolle
  - ○ personelle Maßnahmen ○ organisatorische Maßnahmen
  - ○ technische Maßnahmen

- ☐ 6.9. Benutzerkontrolle
  - ○ personelle Maßnahmen ○ organisatorische Maßnahmen
  - ○ technische Maßnahmen

- ☐ 6.10. Zugriffskontrolle
  - ○ personelle Maßnahmen ○ organisatorische Maßnahmen
  - ○ technische Maßnahmen

- ☐ 6.11. Übermittlungskontrolle
  - ○ personelle Maßnahmen ○ organisatorische Maßnahmen
  - ○ technische Maßnahmen

- ☐ 6.12. Eingabekontrolle
  - ○ personelle Maßnahmen ○ organisatorische Maßnahmen
  - ○ technische Maßnahmen

- ☐ 6.13. Auftragskontrolle
  - ○ personelle Maßnahmen ○ organisatorische Maßnahmen
  - ○ technische Maßnahmen

- ☐ 6.14. Transportkontrolle
  - ○ personelle Maßnahmen ○ organisatorische Maßnahmen
  - ○ technische Maßnahmen

☐ 6.15. Organisationskontrolle
○ personelle Maßnahmen ○ organisatorische Maßnahmen
○ technische Maßnahmen

☐ 6.16. Zusammenfassende Bewertung:
Ausreichend und angemessene Maßnahmen gegen die Beeinträchtigung schutzwürdiger Belange der Betroffenen vorgesehen?

☐ 6.17. Erfolgte Stichprobenkontrolle (Was ist das Ergebnis)?

Anmerkungen:

Zulässigkeit der Verarbeitung personenbezogener Daten auf MS-DOS-PC

Die Verarbeitung personenbezogener Daten mit MS-DOS-Personalcomputern birgt in sich erfahrungsgemäß besondere Risiken, auf die nachfolgend eingegangen wird.

Zulässigkeit nur bei Erfüllung folgender Voraussetzungen:

☐ 7.1. Zugang nur Befugten möglich?
☐ 7.2. Benutzung nur über Paßwort mit Paßwortsicherung?
☐ 7.3. Zwangsweise Menüführung für Zugriff auf aufgabenbezogene Daten?
☐ 7.4. Erfassung der Benutzeraktivitäten in Protokolldatei, die nicht zur Leistungskontrolle benutzt werden darf?
☐ 7.5. Überwachung der ordnungsgemäßen Anwendung der Programme?
☐ 7.6. Sichere Aufbewahrung der Datenträger (Disketten...)?
☐ 7.7. Nachweisführung über den Verbleib der Datenträger?
☐ 7.8. Kontrolle der Einhaltung der obigen Voraussetzungen durch unabhängigenSystemverwalter in Zusammenwirken mit dem internen Datenschutzbeauftragten?

Anmerkungen:

Besondere Maßnahmen zum Schutz personenbezogener Daten in nicht-automatisierten Dateien nach § 9 Abs. 4 SächsDSG

☐ 8.1. Wie wird bei der *Bearbeitung* der Zugriff Unbefugter verhindert?
☐ 8.2. Wie wird bei der *Aufbewahrung* /Archivierung der Zugriff Unbefugter verhindert?
☐ 8.3. Wie wird bei dem *Transport* ein Zugriff Unbefugter verhindert?
☐ 8.4. Wie wird bei der *Aussonderung/Vernichtung* ein Zugriff Unbefugter verhindert? (Vernichtung nach DIN 32 757)

Mängel/Maßnahmen/Termine

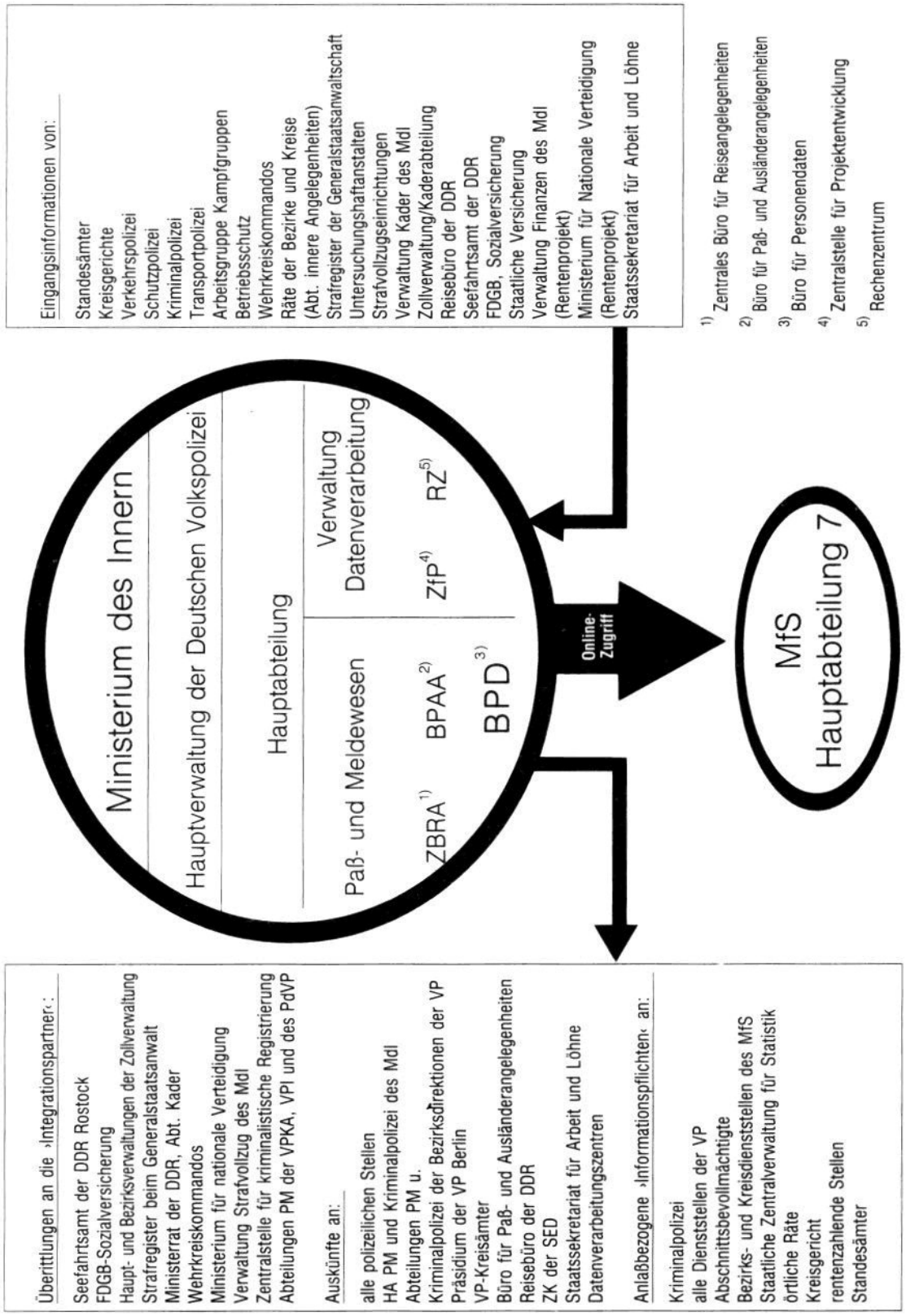
Nr.	*festgestellte Mängel*	*Empfehlung/Maßnahme*	*Termin*
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

Offene Probleme/ ihre Klärung/Termine

Nr.	*Probleme*	*Klärung/Maßnahme*	*Termin*
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			

16.3.2 Personendatenbank des BDP (=Informanten und Nutzer des Zentralen Einwohnerregisters der DDR), aus dem 1. Tätigkeitsbericht des Brandenburgischen Datenschutzbeauftragten

Personendatenbank des BPD [3] - Herzstück des personenbezogenen Datenflusses in der DDR:



16.3.3 Muster für die Datei- und Gerätebeschreibung gemäß § 10 SächsDSG Stand: März 1993

Bezeichnung der datenverarbeitenden Stelle

Behördeninterner Datenschutzbeauftragter

Abteilung/Amt

Telefon

Telefax

---

1. Bezeichnung der Datei und Zweckbestimmung

2. Aufgabe und Rechtsgrundlagen der Verarbeitung

3. Art der gespeicherten Daten

4. Betroffener Personenkreis

Weitere Angaben ☐ in gesonderter Anlage

5. Regelmäßig zu übermittelnde und zu empfangende Daten

5.1 Regelmäßig zu übermittelnde Daten

Art	Empfänger

Weitere Angaben ☐ in gesonderter Anlage

5.2 Regelmäßig zu empfangende Daten

Art	Empfänger

Weitere Angaben ☐ in gesonderter Anlage

6. Sperrungs- bzw. Löschungsfristen

(z. B. nach Abschluß des Verwaltungsverfahrens, nach Einspeicherung oder Ereignis, Differenzierungen)

Dauer der Speicherung geregelt durch:

6.1 Prüfung der Fristen

Wann:

7. Zugriffsberechtigte Personen oder Personengruppen

Weitere Angaben ☐ in gesonderter Anlage

8. Personelle, technische und organisatorische Maßnahmen gemäß § 9 SächsDSG

Dienstanweisung:

Maßnahmen:

9. Bei automatisierten Verfahren

Betriebsart: _____

Art der Geräte: _____

Übermittlungsverfahren: _____

Verfahren zur Sperrung: _____

Verfahren zur Löschung: _____

Auskunftserteilung: _____

10. Automatisierte Datenverarbeitung

Typ: _____ Art: _____

Hersteller: _____ Gerätenummer: _____

Betriebssystem: _____

Möglichkeiten zur
Datenfernverarbeitung: _____

Datenübertragung: _____

16.3.4 Empfehlungen des Sächsischen Datenschutzbeauftragten zur Paßwortgestaltung

Stand: März 1993

Bei der Vergabe von Paßwörtern sind folgende Sicherheitsgrundsätze zu beachten:

1. Jede Person erhält eine eigene Benutzerkennung, die mit einem Paßwort zu schützen ist.
2. Paßwörter dürfen nur dem Benutzer bekannt sein (selbst vergeben, selbst ändern, nirgends notieren, niemandem mitteilen).
3. Als Mindestlänge von Paßwörtern sind sechs Stellen (für Systemverantwortliche acht Stellen) vorzusehen.
4. Der gesamte verfügbare Zeichenvorrat ist auszuschöpfen (Buchstaben, Ziffern, Sonderzeichen).
5. Das Paßwort darf sich nicht auf den Paßwortinhaber beziehen (Name, Vorname, Freundin usw.).
6. Trivialpaßwörter und Paßwörter, die sich aus nebeneinander liegenden Tasten ergeben, sind zu vermeiden (Test, 12345, Asterix, Giesen usw.).
7. Das Paßwort muß einwegverschlüsselt abgelegt werden.
8. Paßwörter dürfen nicht auf Funktionstasten gelegt werden.
9. Ein Paßwortwechsel ist vorzusehen:
   - turnusmäßig (etwa alle zwei Monate),
   - sofort nach Bekanntwerden des Paßworts,
   - nach Wartungsarbeiten.

   Das neue Paßwort darf mit dem alten nicht identisch sein.
10. Es ist festzulegen, wie zu verfahren ist, wenn ein Benutzer sein Paßwort vergessen hat.
11. Das Paßwort des Systemverantwortlichen ist für den Vertretungsfall versiegelt aufzubewahren.
12. Das Paßwort ist gegen Ausprobieren durch Begrenzung der Fehlversuche zu schützen.