



# HESSISCHER LANDTAG

8. Wahlperiode · Drucksache 8/438

26. 03. 75

## **Vorlage des Datenschutzbeauftragten betreffend den Vierten Tätigkeitsbericht**

Mit Schreiben vom 26. März 1975 legt der Datenschutzbeauftragte gemäß § 14 Abs. 1 des Datenschutzgesetzes vom 7. Oktober 1970 (GVBl. I S. 625) dem Landtag den folgenden Vierten Tätigkeitsbericht vor:

Eingegangen am 26. März 1975

Ausgegeben am 23. April 1975

Druck Carl Ritter & Co. Wiesbaden · Vertrieb: Verlag Dr. H. Heger 53 BN-Bad Godesberg Goethestr. 56 Tel. (02221)/365351



**Vierter Tätigkeitsbericht  
des  
Hessischen Datenschutzbeauftragten**

**vorgelegt zum 31. März 1975**

**gemäß § 14 des Hessischen Datenschutzgesetzes**

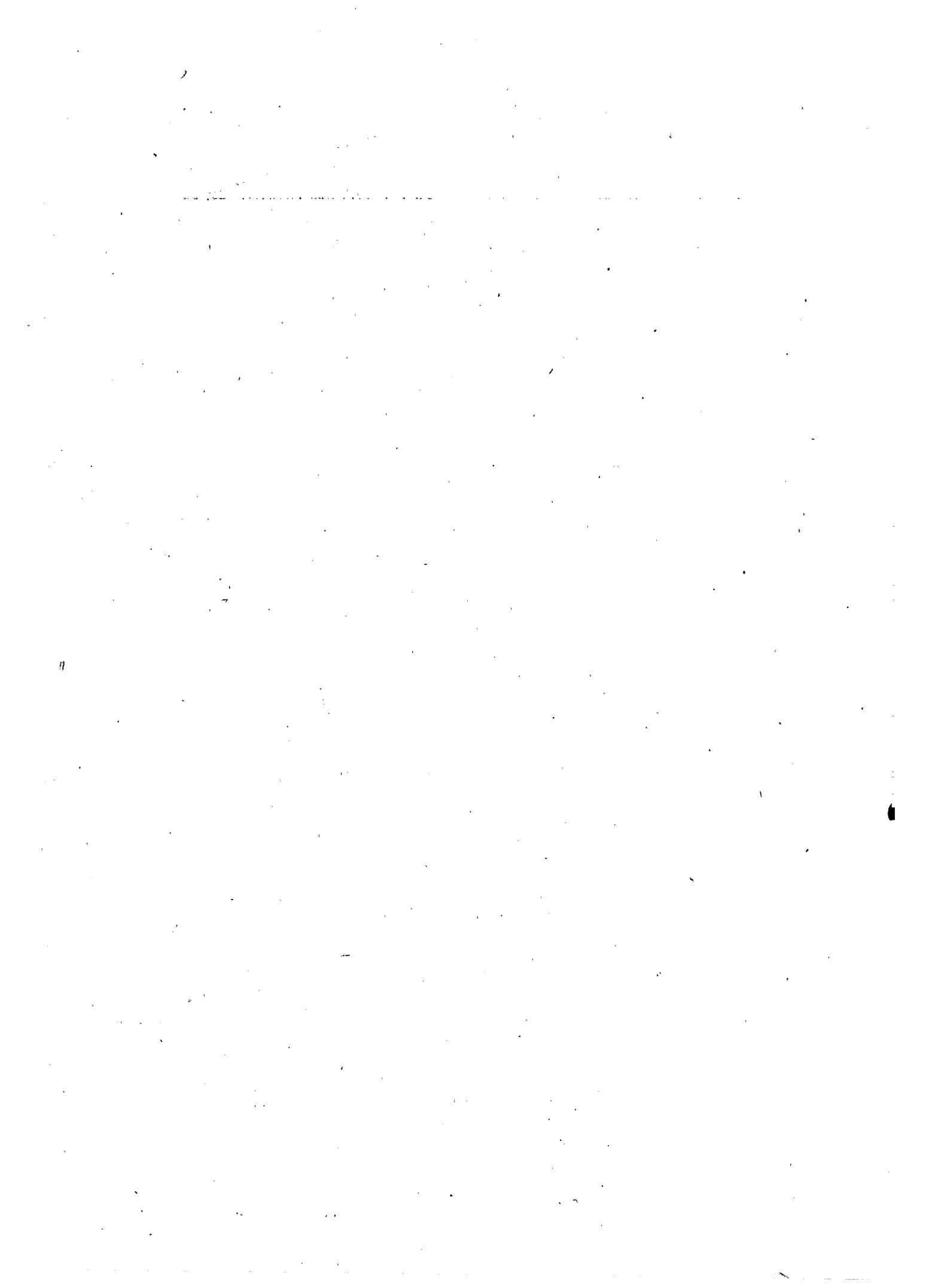
**vom 7. Oktober 1970**



# INHALTSVERZEICHNIS

	Seite
1 Bilanz nach vierjähriger Datenschutzpraxis .....	7
1.1 EDV-Ausschuß des Landtags .....	7
1.2 Fairness-Kodex und Datenverkehrs-Ordnung .....	7
1.3 Internationales Zusammenwirken .....	7
1.4 Informationsgespräche .....	7
1.5 Anpassung des hessischen Gesetzes .....	8
1.5.1 Allgemeine Grundsätze .....	8
1.5.2 Spezielle Regelungen .....	9
1.5.3 Gefahrenabwehr .....	9
1.6 Eingaben an den Datenschutzbeauftragten .....	9
1.7 Bemerkungen zu den Befragungen .....	10
2 Gesetzgebungsstand ausserhalb Hessens .....	11
2.1 Bundesmeldegesetz und Bundesdatenschutzgesetz .....	11
2.2 Ausland .....	11
2.2.1 Europarat, Europäische Gemeinschaften, OECD .....	11
2.2.2 Die Schwedische Datainspektionen .....	11
2.2.3 Das US-Datenschutzgesetz von 1974 .....	12
3 Datenbankregister .....	13
3.1 Datenartenkatalog .....	13
3.2 Protokollierung .....	15
4 Tätigkeiten des Datenschutzbeauftragten .....	17
4.1 Präventives Wirken .....	17
4.2 Datenschutz in Rechenzentren .....	17
4.3 Mitarbeit in Verwaltungsausschüssen .....	18
4.4 Datenfernverarbeitung im Einwohnermeldewesen .....	18
4.5 Informationssysteme bei Verfassungsschutz und Polizei .....	19
4.5.1 Zusammenarbeit mit anderen Ländern und Bund .....	19
4.5.2 Regelung in HEPOLIS .....	20
4.6 Weitergabe von Einzelangaben aus Bundesstatistiken .....	20
4.7 Datenschutz in Individualdateien und bei Sondererhebungen .....	20
4.7.1 Schulsportärztlicher Untersuchungsbogen .....	20
4.7.2 Gesundheitsdatenbanken .....	20
4.7.3 Schülerindividualdateien .....	21
4.7.4 Studentendateien .....	21
4.7.5 Forschungstests an Schulen .....	21
4.7.6 Unterrichtung des Datenschutzbeauftragten .....	21
4.7.7 Umgang mit Individualdaten .....	22
4.7.8 Datenweitergabe für gewerbliche Zwecke .....	22
5 Sicherung des Informationsgleichgewichts .....	23
5.1 Zugriffsrechte des Parlaments .....	23
5.1.1 Ergänzungen des § 6 DSG .....	23
5.1.2 Verhältnis Parlament und HEPAS .....	23
5.1.3 Informationen aus Statistiken .....	23
5.1.4 Datenbestände des Landes .....	24
5.1.5 Auch Bundestag prüft Zugriffsrechte .....	25
5.1.6 Weitergabe von Adressen an Parteien .....	25
5.2 HEPAS-Land und HEPAS-Kommunal .....	25
6 Schlussbemerkungen .....	27
Anlage 1: Datenverkehrsordnung .....	29
Anlage 2: Sachverständigenanhörung des Bundestags-Innenausschusses .....	31
Sachwörterverzeichnis .....	35

Bei den Hinweisen bezeichnen I, II und III den Ersten, Zweiten bzw. Dritten Tätigkeitsbericht; die arabischen Ziffern die Abschnitte der Berichte.



# 1. BILANZ NACH VIERJÄHRIGER DATENSCHUTZPRAXIS

## 1 Bilanz nach vierjähriger Datenschutzpraxis

Dem Berichtszeitraum des Vierten Tätigkeitsberichtes haben der Ablauf der Legislaturperiode des 7. und die Konstituierung des 8. Hessischen Landtags besondere Akzente gegeben.

### 1.1 EDV-Ausschuß des Landtags

Der scheidende Landtag hat in einer seiner letzten Sitzungen beschlossen, die Empfehlungen der Arbeitsgruppe elektronische Datenverarbeitung (EDV) seines Hauptausschusses dem neuen Landtag zur Verfügung zu stellen. Diesem wurde es damit ermöglicht, die Anregungen und Empfehlungen aus den drei Tätigkeitsberichten des Datenschutzbeauftragten und die Stellungnahmen der Landesregierung weiter zu behandeln, ohne daß sie erneut eingebracht werden mußten.

Der neue Landtag hat sich mit der Einsetzung eines Fachausschusses für elektronische Datenverarbeitung ein Organ geschaffen, das sich mit den Vorschlägen und Anregungen des Datenschutzbeauftragten intensiv befassen und die EDV den Bedürfnissen des Parlaments nutzbar machen kann. Die Zuständigkeit des Hauptausschusses für grundlegende Verfassungsfragen und die von der Materie her gegebenen Mitwirkungsrechte anderer Fachausschüsse bleiben dabei unberührt.

### 1.2 Fairness-Kodex und Datenverkehrs-Ordnung

Mit den Vorschlägen für einen „Fairness-Kodex für den Umgang mit Informationen“ und für eine „Datenverkehrs-Ordnung für die EDV“ bei der förmlichen Einbringung des Dritten Tätigkeitsberichts im Landtagsplenum am 28. 8. 1974<sup>1)</sup> hat der Datenschutzbeauftragte seinerseits eine Zusammenfassung der grundlegenden Regeln für den Datenschutz vorgelegt, die in den ersten drei Tätigkeitsberichten und in zahlreichen anderen Verlautbarungen aufbereitet und an Hand von Beispielen erläutert worden sind.

Diese Regeln sind ihrem Inhalt nach weitgehend unbestritten. In wissenschaftlichen Veröffentlichungen sind gleiche Gedanken erörtert worden; sie haben auch in Gesetzen und in Gesetzentwürfen anderer Länder ihren Niederschlag gefunden. Eine Synopse der Datenschutzvorschriften, die in anderen Bundesländern und in anderen Staaten erlassen oder geplant sind, würde eine vielfältige Übereinstimmung mit dem Hessischen Datenschutzgesetz und vor allem auch mit den Forderungen und Anregungen des Datenschutzbeauftragten für Maßnahmen und Vorkehrungen eines praktizierten Datenschutzes aufzeigen.

Ein Beispiel aus jüngster Zeit ist hierfür das US-Datenschutzgesetz, der „Privacy Act of 1974“, der Ende

1974 vom amerikanischen Kongreß beschlossen und am 1. 1. 1975 vom Präsidenten der USA in Kraft gesetzt worden ist. Die dort zu findenden Parallelen zum hessischen Gesetz und zu den Beiträgen des Hessischen Datenschutzbeauftragten sind u. a. auch Ausflüsse des Erfahrungsaustauschs, den der Datenschutzbeauftragte während eines Amerika-Aufenthaltes im Jahre 1972 und anschließend schriftlich mit den für die Datenschutzregelung maßgebenden Stellen in den Vereinigten Staaten gepflogen hat und weiter unterhält.

Im übrigen kann aus den zahlreichen Aufforderungen zur Mitwirkung an Beratungen, Diskussionen, öffentlichen Anhörungen, Interviews und sonstigen Veröffentlichungen abgelesen werden, daß die Institution des Hessischen Datenschutzbeauftragten als ein beispielhaftes Modell für den öffentlichen Bereich anerkannt worden ist. Dieses positive Ergebnis rechtfertigt den erstmals vom Lande Hessen eingeschlagenen Weg, mit der Anwendung der EDV in der öffentlichen Verwaltung zugleich den Datenschutz zu realisieren.

### 1.3 Internationales Zusammenwirken

Der Datenschutzbeauftragte hat von vornherein seine Aufgabe nicht als eine partikuläre Landesaufgabe verstanden, sondern versucht, ein Modell aufzubauen, das bei der Bewältigung der vielschichtigen Datenschutzprobleme zu einer Gemeinsamkeit mit den anderen Ländern der Bundesrepublik führt.

Der Datenschutz ist darüber hinaus nicht nur eine deutsche, sondern eine internationale Aufgabe. Die nationalen Grenzen sind schon wegen der starken internationalen Wirtschaftsverflechtung keine Schranke gegen den Datenfluß und gegen Datenmißbräuche. Daher hat sich der Datenschutzbeauftragte auch an Diskussionen und Beratungen über Datenschutzprobleme in internationalen Gremien, zu denen er eingeladen worden ist, beteiligt, z. B. an Veranstaltungen der OECD und des Europarates. Obwohl die gesetzliche Grundlage nur das Landesgesetz ist, ist es gelungen, die sich in Hessen stellenden Datenschutzfragen in einem übernationalen Zusammenhang zu aktualisieren.

### 1.4 Informationsgespräche

Längere Informationsgespräche führte der Hessische Datenschutzbeauftragte in Wiesbaden u. a. mit Fachleuten — teils aus der Wissenschaft, teils aus der Verwaltung oder der Datenverarbeitungspraxis — aus den Niederlanden, aus Japan, der Schweiz und Norwegen. Darüber hinaus bestand ein reger schriftlicher Austausch mit weiteren Ländern, u. a. mit Großbritannien, Kanada, Neuseeland, Österreich und Frankreich. Bei den Gesprächen mit den Vertretern aus Japan fiel auf, daß sich dort nicht nur staatliche Stellen, wie die japanische Postverwaltung, für den Daten-

<sup>1)</sup> Stenographischer Bericht 7/97 vom 28. 8. 1974, s. 5227f., siehe auch Anlage I

schutz interessieren. Auch die Gewerkschaften, die eine Delegation nach Wiesbaden entsandt hatten, messen den Problemen des Datenschutzes große Bedeutung zu.

Mitte Oktober 1974 fand ein mehrtägiger Erfahrungsaustausch zwischen den beiden einzigen bisher auf dem Gebiet des Datenschutzes tätigen unabhängigen Institutionen, der schwedischen Datainspektionen und dem Hessischen Datenschutzbeauftragten, statt.

Dieser Erfahrungsaustausch hat gezeigt, daß trotz des Unterschiedes bei Rechtsbasis und Vollmachten die schwedische Datainspektionen und der Hessische Datenschutzbeauftragte zum großen Teil durch gleichartige Maßnahmen den Mißbrauch personenbezogener Daten zu verhindern suchen. Schwerpunkte des Gesprächs waren vor allem Probleme, die im Zusammenhang mit polizeilichen und medizinischen Informationssystemen auftauchen. In allen grundsätzlichen Fragen ergab sich volle Übereinstimmung.

Inzwischen wurde der Erfahrungsaustausch zwischen beiden Datenschutzinstitutionen durch den gegenseitigen Austausch von Gutachten, Veröffentlichungen, Aufsätzen und — seitens der Datainspektionen — von Beschlüssen zur Genehmigung von Datenbanken fortgesetzt. Von besonderem Interesse ist die Einschätzung einer Gefährdung des Persönlichkeitsrechts durch entstehende (oder in Schweden bereits existierende) private zentrale Personenregister (vgl. unter 2.2.2).

Diese Ausweitung der Aktivitäten des Datenschutzbeauftragten hat sich auf das Verständnis für die Erfordernisse des Datenschutzes im eigenen Lande im gesamten Umfange der in § 10 des Hessischen Datenschutzgesetzes (DSG) formulierten Aufgaben befruchtend ausgewirkt.

## 1.5 Anpassung des hessischen Gesetzes

In der öffentlichen Verwaltung ist ein stetiger Prozeß der Verwirklichung von Datenschutzgrundsätzen in Gang gesetzt worden (vgl. III, 1.5). Die steigende Bereitschaft der meisten Behörden und Stellen der öffentlichen Verwaltung, die Forderung des Datenschutzbeauftragten zu akzeptieren, ist um so bemerkenswerter, als das Gesetz keine konkreten Maßnahmen für die Verwirklichung des Datenschutzes vorschreibt. Vielmehr hat erst der Datenschutzbeauftragte Maßstäbe für den Vollzug des Gesetzes entwickeln müssen. Hierbei hat er sich an der wissenschaftlichen Aufbereitung der Datenschutzprobleme und an der Entwicklung in anderen Ländern und Staaten orientiert (vgl. unter 2). Die Forderungen des Datenschutzbeauftragten sind so zwar durch Praxis und Wissenschaft abgesichert, jedoch im Gesetz nur in den Generalklauseln der §§ 2 und 10 normiert.

Diese Situation ist unbefriedigend. Der Bürger und auch die Behörden und Stellen der öffentlichen Verwaltung können in vielen einzelnen Fällen nicht mit hinreichender Gewißheit dem Gesetz entnehmen, ob eine beabsichtigte Datenverarbeitung — vornehmlich eine Datenweitergabe — zulässig ist. Diese Unsicherheit führt zu der die Funktionen des Datenschutzbe-

auftragten sinnwidrig verändernden Forderung, er möge entscheiden, wie sich die Verwaltung verhalten solle und welche Maßnahmen im Einzelfall oder in einzelnen Verwaltungsautomationsverfahren dem gesetzlich verordneten Datenschutz genügen. Man versucht, die Verantwortung dafür, daß und in welcher Weise Datenschutz zu verwirklichen ist, dem Datenschutzbeauftragten zuzuschreiben, so als ob er eine parlamentarisch verantwortliche Aufsichtsbehörde wäre (vgl. unter 4.3).

Diese Erfahrung unterstreicht die Notwendigkeit, die Anpassung der Praxis an die anerkannten Erfordernisse des Datenschutzes nunmehr gesetzlich zu vollziehen, indem die für den Datenschutz geltenden Grundregeln in Rechtsnormen festgelegt werden. Sowohl dem Bürger als auch der Verwaltung würden damit sichere Maßstäbe an die Hand gegeben, an denen geprüft werden kann, ob Verfahren und Verhaltensweisen der Verwaltung im einzelnen Fall den Erfordernissen des Datenschutzes entsprechen.

### 1.5.1 Allgemeine Grundsätze

Aus der bereits erwähnten Datenverkehrs-Ordnung für die EDV<sup>2)</sup> könnten die wesentlichen Grundsätze abgeleitet werden, mit denen das Datenschutzgesetz vom 7. 10. 1970 aufgefüllt werden sollte.

In Stichworten handelt es sich vor allem um folgende Forderungen an die öffentliche Verwaltung:

- 1) Die Verwaltung soll bekanntgeben, welche Datenarten für welche Verwaltungsaufgaben oder sonstige Zwecke sie sammelt.
- 2) Die Verwaltung soll dem Bürger Auskunft über den Inhalt der über ihn gespeicherten Daten geben, soweit dies nicht gesetzlich ausgeschlossen ist. Ohne ein Auskunftsrecht ist der Berichtigungsanspruch nach § 4 DSG nicht zu verwirklichen. Als Wegweiser für den Bürger könnte ein sogenanntes Datenbankregister (vgl. unter 3.1) dienen, das beim Datenschutzbeauftragten für jedermann zur Einsicht ausliegt.
- 3) Bei der Erhebung von Daten soll die Verwaltung dem Befragten die Rechtsgrundlagen nennen, auf denen seine Auskunftspflicht beruht; falls er zur Auskunft nicht verpflichtet ist, soll die Verwaltung ihn über sein Recht, die Auskunft zu verweigern, belehren.
- 4) Für den Erhebungszweck nicht mehr erforderliche Daten sind zu löschen oder in anderer Weise aus dem Datenverarbeitungssystem zu entfernen (sperrern).

Die vorgenannten Maßnahmen sind Beispiele für ein Datenschutz-Instrumentarium, das dem Schutz des Persönlichkeitsrechts des Bürgers unmittelbar dient. Die Verwaltung ist jedoch zu weiteren Maßnahmen zu verpflichten, die in erster Linie der Sicherung der Datenverarbeitung und damit der Erfüllung der Verwaltungsaufgaben zugleich aber auch dem Schutz des Bürgers vor Mißbrauch seiner Daten dienen. Hierzu gehören u. a. die Abschirmung der Daten und der

<sup>2)</sup> Siehe Anlage I

Programme gegen äußere Eingriffe, die Kontrolle des Programmablaufs durch Protokollierung, technische Zugriffssperren und weitere Vorkehrungen, wie sie z. B. in den Richtlinien zur Gewährleistung des Datenschutzes und der Datensicherheit im Datenverarbeitungs-Verbund Hessen (DASCH) vorgesehen sind.

### 1.5.2 Spezielle Regelungen

Da sowohl das Schutzbedürfnis des Bürgers gegen mißbräuchliche Verwendung seiner Daten als auch der Zweck der Verwaltungsaufgabe, der die EDV dient, in den Ressort-Bereichen untereinander verschieden sind und spezielle Regelungen erfordern, kann in einem allgemeinen Datenschutzgesetz nur ein Grundsatz-Rahmen festgelegt werden. Der Rahmen müßte von Regelungen ausgefüllt werden, welche den unterschiedlichen Ressort-Aufgaben angepaßt sind. So erfordern z. B. das Einwohnerwesen, das Gesundheitswesen, das kriminalpolizeiliche Informationssystem und dgl. voneinander abweichende Datenschutz-Maßnahmen. Den spezifischen von der EDV ausgehenden Gefährdungen kann nur mit Maßnahmen begegnet werden, die den verschiedenartigen Situationen im Verhältnis des Bürgers zur Verwaltung entsprechen. Dies beginnt schon bei der Amtshilfe, die nicht in jedem Bereich der automatisierten Verwaltung gleichartig gewährt werden darf (vgl. unter 4.6). Die Vorstellung von der Einheit der Verwaltung ist durch Arbeitsteilung und Spezialisierungen in den einzelnen Zweigen der Verwaltung und durch ihren wachsenden, den Bürger immer eindringlicher erfassenden Informationsbedarf strittig geworden (vgl. unter 4.4 bis 4.7).

So läßt die Vorschrift, daß das Land Hessen Zugriff zu „seinen“ Datenbeständen hat (§§ 3–5 Datenverarbeitungsgesetz – DVG –) völlig offen, welche Behörde oder Stelle des Landes im Einzelfall zugriffsberechtigt und ob die Zuständigkeitsregelung der Landesregierung nach Art. 104 Abs. 2 HV einschlägig und ausreichend ist.

Ein allgemeines Datenschutzgesetz genügt daher nicht; es bedarf der Ergänzung durch spezielle, ressort- oder aufgabenbezogene Rechtsnormen, sei es in Spezialgesetzen wie etwa in dem Hessischen Krankenhausgesetz, sei es durch Rechtsverordnungen, zu denen das Rahmengesetz ermächtigt.

Parallel zu einer solchen Anpassung des geltenden Datenschutzgesetzes an die Erfordernisse der Verwaltungswirklichkeit müssen die Kontrollbefugnisse des Datenschutzbeauftragten erweitert werden, wie es bereits im Dritten Tätigkeitsbericht (vgl. III, 1.5.1) gefordert worden ist.

Für die gesetzliche Ausgestaltung einer solchen Novellierung liefern die Diskussionen um die entsprechenden Bestimmungen im Regierungsentwurf eines Bundesdatenschutzgesetzes vielfältiges Material.

### 1.5.3 Gefahrenabwehr

Die Technik der Datenverarbeitung und deren Mittel befinden sich in einer stetigen, teilweise sprunghaften Entwicklung. Der Datenschutz muß daher den sich verändernden Situationen ständig angepaßt werden.

Daneben sind auch gesellschaftspolitische Veränderungen im Staatsverständnis und im Selbstverständnis gesellschaftlicher Gruppen – wenn sich diese auch wesentlich langsamer vollziehen – zu berücksichtigen. Beispiele sind die Entwicklung der Eingriffs-Verwaltung zur Leistungs-Verwaltung, die zunehmende Arbeitsteilung durch Spezialisierungen, und die Verwirklichung des Demokratiegebotes durch verstärkte Mitwirkungsrechte gesellschaftlicher Gruppen. Dadurch, daß die Institution Datenschutz diese Tendenzen und die Entwicklungen auf dem Gebiete der Technik in ihre Betrachtungen einbezieht, soll eine vor allem präventive, künftige Gefahren abwehrende Wirkung erreicht werden. In dieser Zielsetzung unterscheidet sich der Datenschutz grundsätzlich von anderen vergleichbaren Einrichtungen des Rechtsstaates, wie z. B. der Rechtsweggarantie.

Es wäre daher verfehlt, die Datenverarbeitung in der hessischen öffentlichen Verwaltung sich fortschreitend entwickeln zu lassen, ohne zugleich den grundsätzlich für notwendig erkannten Datenschutz auch rechtlich abzusichern. Für beginnende mißbräuchliche Verwendungen personenbezogener Daten sind in diesem und in den vorausgehenden Tätigkeitsberichten bezeichnende Beispiele aufgeführt. Aus vielfältigen Erfahrungen in anderen Lebensbereichen weiß man, daß die Mißbrauchsgefahren wachsen, je größer die finanziellen und personellen Investitionen für die „gefährlichen Anlagen“ sind und je später Abwehrmaßnahmen ergriffen werden. Es könnte verhängnisvoll werden, wenn das zeitlich ungewisse Inkrafttreten eines Bundesdatenschutzgesetzes abgewartet werden und der rechtzeitige Ausbau eines effizienten Datenschutzes in Hessen parallel zu der fortschreitenden Einführung der EDV vernachlässigt würde. Zweifel an der Gesetzgebungs-Kompetenz schlagen nicht durch. Die nachstehenden Beispiele (vgl. unter 4.4 bis 4.7) zeigen, daß das Persönlichkeitsrecht des Bürgers gefährdet ist und daß Informationsmonopole besonders im Bereich der gesetzefreien Verwaltung – Landesentwicklungsplanungen, Personalverwaltung und dgl. – möglich sind.

### 1.6 Eingaben an den Datenschutzbeauftragten

Im Berichtszeitraum haben sich wesentlich mehr Bürger an den Datenschutzbeauftragten gewandt und ihn von Datenverarbeitungsfällen unterrichtet, die sie als Belästigung und unbefugtes Eindringen in ihre Privatsphäre empfanden. Mit dem Vordringen der Datenverarbeitung in immer neue Lebensbereiche sind für viele Bürger neue Situationen entstanden, in denen sie Hilfe, mindestens Auskünfte bei einer neutralen Stelle suchen. Deshalb wenden sie sich an den Datenschutzbeauftragten, dessen Funktion offensichtlich immer stärker in das Bewußtsein der Öffentlichkeit getreten ist. In vielen dieser Eingaben wurde auf den Handel mit Adressen verwiesen, die offensichtlich aus Dateien der öffentlichen Verwaltungen und der Hochschulverwaltung stammen, sowie auf eine Reihe von Schülerbefragungen. Diese Befragungsaktionen an Schulen sind besonders erwähnenswert. Die Fragen bezogen sich u. a. auf den sozialen Status der Eltern und auf das Verhältnis der Kinder zu ihren Eltern; sie hatten

ferner eine Beurteilung des Vaters und der Mutter durch das Kind zum Inhalt usw. ~~In anderen Fällen~~ wurden die Leistungsdaten der Schüler zusammen mit den Angaben über die soziale Herkunft und Ausbildung der Eltern, deren Beruf, über die Familienverhältnisse, politische Einstellungen und religiöse Bekenntnisse erfaßt oder nach „polizeilich unentdeckten Straftaten“ des Schülers vor dem 14. Lebensjahr.

#### 1.7 Bemerkungen zu den Befragungen

Bei diesen Vorgängen im hessischen Schulbereich handelt es sich nicht um Einzelfälle. An zahlreichen Hochschulen bilden sich Gruppen, die die Möglichkeiten des Computers für wissenschaftliche oder Verwaltungsvorhaben zu nutzen suchen. Die gleichen Vorgänge sind übrigens auch in den Nachbarländern zu beobachten.

Forschungsvorhaben sind für die pädagogische Arbeit und für die Verbesserung von Lehrmethoden von großer Bedeutung. Ihre grundsätzliche Notwendigkeit wird niemand ernsthaft bestreiten können; zu bemängeln wäre es aber, wenn dabei Daten von einer allgemein hohen Empfindlichkeitsstufe namentlich erfaßt und gespeichert würden oder wenn die Anonymisierung so unzureichend erfolgte, daß eine Rückidentifikation durch am Test Beteiligte oder durch Lehrer möglich wäre.

Bei den bekanntgewordenen Befragungsaktionen waren die Bereiche von Forschung und Verwaltung oft nicht klar getrennt, sondern gingen ineinander über oder wurden miteinander vermischt. Es kann nicht ausbleiben, daß in dieser „Grenzzone“ eine Fülle von Datenschutzproblemen entstehen (vgl. unter 4.7.5 bis 4.7.6).

"In anderen Fällen wurden die Leistungsdaten der Schüler zusammen mit Angaben über die soziale Herkunft, Ausbildung und Beruf der Eltern erfaßt oder es wurde nach den Familienverhältnissen, politischen Einstellungen und religiösen Bekenntnissen der Schüler und nach von ihnen vor dem 14. Lebensjahr begangenen "polizeilich unentdeckten Straftaten" gefragt".

## 2. GESETZGEBUNGSSTAND AUSSERHALB HESSENS

### 2 Gesetzgebungsstand außerhalb Hessens

Da in einer Reihe von Bundesländern und in ausländischen Staaten – z. T. seit Jahren – Datenschutz-Gesentwürfe vorliegen, ohne daß abzusehen ist, wann und in welcher Form sie verabschiedet werden, wird in diesem Bericht davon abgesehen, weiterhin Übersichten und Erläuterungen der Entwürfe für Datenschutzgesetze zu geben, es sei denn, sie enthalten neue Anregungen oder Lösungsvorschläge.

#### 2.1 Bundesmeldegesetz und Bundesdatenschutzgesetz

Das Gesetzgebungsverfahren auf Bundesebene hat sich verzögert. Der Innenausschuß hat im Januar den Entwurf des Bundesmeldegesetzes intern verabschiedet. Er wird jetzt den Entwurf des Bundesdatenschutzgesetzes beraten.

Bereits an dem Hearing, das der Bundesinnenminister 1972 veranstaltet hatte, hatte der Hessische Datenschutzbeauftragte als Sachverständiger teilgenommen. Er ist auch aufgefordert worden, bei der Sachverständigenanhörung des Innenausschusses des Bundestages am 6. Mai 1974 zu bestimmten Fragen Stellung zu nehmen. Dabei handelte es sich insbesondere um die Einrichtung eines externen Kontrollorgans für den Datenschutz und um seine organisatorische Gestaltung, seine Ausstattung und seine grundgesetzliche Verankerung. Die schriftlichen Stellungnahmen zu diesen Fragen sind in Anlage II im Wortlaut wiedergegeben (vgl. auch II, Anlage 1).

#### 2.2 Ausland

Mit Ausnahme des US-Datenschutzgesetzes von 1974 (vgl. unter 2.2.2) wurden im Berichtszeitraum in Europa und Übersee keine Datenschutzgesetze verabschiedet. Es sind jedoch einige interessante Entwicklungen zu verzeichnen.

##### 2.2.1 Europarat, Europäische Gemeinschaften, OECD

Eine Experten-Konferenz der OECD hat im Juni 1974 in Paris gemeinsame Fragestellungen zum Datenschutzproblem erarbeitet. Wichtigste Themen waren der Schutz der Privatsphäre, das Informationsgleichgewicht zwischen Exekutive und Legislative und die Organisation der externen Kontrolle. Der Datenschutzbeauftragte hat seine Erfahrungen in diese Diskussionen eingebracht. Im Rahmen der OECD waren bereits Anfang 1972 englische und französische Übersetzungen des Hessischen Datenschutzgesetzes erschienen.

Der Rechtsausschuß des EUROPÄISCHEN PARLAMENTES hat am 19. Februar 1975 einen Zwischenbericht „über den Schutz der Rechte des einzelnen angesichts der fortschreitenden technischen Entwicklung auf dem Gebiet der automatischen Daten-

verarbeitung“ erstellt. Darin wird u. a. ein Entschließungsantrag vorgelegt, der zum Ziele hat, einheitliche Richtlinien über die „Freiheit des einzelnen und die Datenverarbeitung“ für die Staaten der Europäischen Gemeinschaften zu verabschieden.

Der Minister-Ausschuß des EUROPARATES hat am 20. September 1974 eine Resolution (74) 29 über den „Schutz des Persönlichkeitsrechts von einzelnen in elektronischen Datenbanken im öffentlichen Bereich“ angenommen. Die acht Grundsätze dieser Resolution entsprechen im großen und ganzen den in der „Datenverkehrs-Ordnung“ des Hessischen Datenschutzbeauftragten enthaltenen Datenschutz-Grundsätzen; sie haben auch in den neuen Entwurf eines österreichischen Datenschutzgesetzes Eingang gefunden. Es fehlt allerdings die Einbeziehung des Informationsgleichgewichts zwischen Regierung und Parlament. Darauf hat der Hessische Datenschutzbeauftragte bei einer Expertenanhörung des Europarats im Februar dieses Jahres in Straßburg hingewiesen. Seine Anregung wurde vom Generalsekretariat des Europarats sowie den drei teilnehmenden Sachverständigen aus europäischen Nachbarländern mit Interesse aufgenommen.

##### 2.2.2 Die Schwedische Datenspektionen

In Schweden bestand bisher die Übung, daß vom Reichsregister einem bestimmten privaten Unternehmen (X) Bandkopien der jeweils auf den neuesten Stand gebrachten Anschriften aller Bürger, aufgeteilt nach Provinzen, überlassen wurde. Diese Bandkopien ermöglichten es dem Unternehmen X, das Adressen für die Direktklame anbietet, den an Direktwerbung Interessierten nicht nur die gültige Anschrift weiterzugeben. Anhand zusätzlicher Merkmale, wie z. B. Familienstand, persönliches Einkommen, Familieneinkommen und Grundbesitz, war es möglich, jeweils auf die Geschäftsart abzustimmende besondere Untergruppen und Zielgruppen zu bilden.

In unserer Rechtsordnung würde sich die Frage stellen, ob die Weitergabe der personenbezogenen Daten durch eine amtliche Stelle überhaupt zulässig ist. Ein weiteres Problem ergäbe sich aus der Praxis der Direktwerber, bei dem Unternehmen X nur die sie selbst interessierenden Anschriften-Kategorien anzufordern. Durch die zentrale Speicherung der verschiedenen Datenkategorien für die einzelnen Direktwerber bei dem Unternehmen X taucht zwangsläufig als Nebenprodukt für jede gespeicherte Adresse ein „Werbeprofil“ auf, d. h. eine Zusammenfassung aller Merkmale, die für den betroffenen Adresseninhaber aufgrund seines Familienstandes, seines Einkommens, seines Grundbesitzes, seiner Geschäftsinteressen u. a. zutreffen und nach denen er von der Werbung gezielt angesprochen werden kann. Aus diesem Werbeprofil

kann, ergänzt man es durch zusätzliche Informationen, leicht ein Persönlichkeitsprofil entstehen.

Die hier vorhandene Gefahr gilt übrigens auch für die zahlreichen, in der Bundesrepublik existierenden Firmen, die Adressen — aufgliedert nach den verschiedensten Kategorien — für gezielte Werbekampagnen anbieten.

Als das Unternehmen X nach Verabschiedung des schwedischen Datenschutzgesetzes um die Genehmigung zur Weiterführung dieses Registers nachsuchte, hat die Datainspektionen die Gefahr gesehen und die Fortsetzung dieser Praxis des Unternehmens X nur für einen befristeten Zeitraum zugelassen. Sie ordnete an, daß sowohl auf Seiten der Behörden als auch beim Unternehmen Maßnahmen erfolgen, die einen Mißbrauch ausschließen.

### 2.2.3 Das US-Datenschutzgesetz von 1974

In den Vereinigten Staaten war — wie bereits im Dritten Tätigkeitsbericht erwähnt — ein Kabinettsausschuß („Domestic Council Committee on the Right of Privacy“) unter Vorsitz des damaligen Vizepräsidenten Gerald Ford beauftragt worden, Vorschläge für die Gesetzgebung auf dem Gebiet des Datenschutzes zu erarbeiten, nachdem man bereits Erfahrungen mit dem Fair Credit Reporting Act vom April 1971 (FCRA), das den Datenschutz für den Bereich der Kreditauskunfteien regelt, gesammelt hatte.

Da der Fair Credit Reporting Act nur für einen bestimmten Teil des nicht-staatlichen Bereichs gilt, bestand das vordringliche Bedürfnis für eine Datenschutzregelung im öffentlichen Bereich fort.

Dem trägt das Datenschutzgesetz von 1974 Rechnung: Es unterwirft den Bereich der Bundesverwaltung detaillierten Datenschutzbestimmungen (Artikel 2 (b) des Gesetzes). Daneben enthält es einige auch für bundesstaatliche und Kommunalbehörden geltende Bestimmungen (Artikel 7); darüber hinaus trifft es Vorsorge, künftig weitere Bereiche der öffentlichen Verwaltung sowie der Privatwirtschaft zu erfassen (Artikel 5). Beachtenswert ist ferner, daß das amerikanische Gesetz die nachrichtendienstlichen und polizeilichen Informationssysteme nicht völlig ausnimmt, sondern nur von bestimmten Auflagen freistellt (Artikel 3 (j) (1) (2) (k) (2) (3) ).

Für die hessische Konzeption des Datenschutzes sind folgende Vorschriften von besonderem Interesse:

Die Frage des Informationsgleichgewichts zwischen den Staatsgewalten, die zuerst im Hessischen Datenschutzgesetz vom 7. Oktober 1970 Eingang in eine

gesetzliche Regelung gefunden hat, ist durch die Aufnahme in das amerikanische Datenschutzgesetz erneut als regelungsbedürftig hervorgehoben worden.

Die Vorschrift in Art. 3 §§ 552 a (o) lautet:

„Jede Behörde soll dem Kongreß und dem Office of Management and Budget hinreichend frühzeitig über Vorschläge zur Errichtung oder Änderung von Datenbanken Mitteilung machen, damit die Möglichkeit gegeben ist, die wahrscheinlichen oder möglichen Auswirkungen solcher Vorschläge auf das Persönlichkeitsrecht und andere persönliche oder Eigentumsrechte von einzelnen oder auf die Weitergabe von auf solche einzelnen bezügliche Information und die Auswirkung auf die Erhaltung der verfassungsmäßigen Grundsätze des Föderalismus und der Gewaltenteilung auszuwerten.“

Das Prinzip der „externen Kontrolle“, auf dem die Einrichtung des Hessischen Datenschutzbeauftragten beruht, wird auch im US-Gesetz verwirklicht, allerdings in anderer organisatorischer und funktionaler Gestaltung und auf die Zeit von zwei Jahren begrenzt. Artikel 5 sieht die Einrichtung einer Kommission zum Schutze des Persönlichkeitsrechts vor. Ihre Aufgabe ist es, umfassende Untersuchungen der Datenbanken, automatisierten Datenverarbeitungsprogramme und Informationssysteme von Regierungs-, regionalen und privaten Organisationen vorzunehmen, um die in Kraft befindlichen Grundsätze und Verfahren für den Schutz personenbezogener Informationen zu erforschen und um zu ermitteln, in welchem Umfang Regierungs- und private Informationssysteme die Beziehungen zwischen Bund und Bundesstaaten oder den Grundsatz der Gewaltentrennung beeinträchtigen. Hierüber hat die Kommission die Regierung und den Kongress zu unterrichten und zu beraten.

Die Kommission setzt sich aus drei vom Präsidenten der Vereinigten Staaten, zwei vom Präsidenten des Senats und zwei vom Speaker des Repräsentantenhauses ernannten Mitgliedern zusammen. Ihre Befugnisse sind sehr weitgehend. Sie kann z. B. Zeugen anhören und vereidigen, durch Ordnungsstrafen deren Erscheinen oder die Vorlage von Beweismaterial erzwingen und vertragliche Vereinbarungen mit staatlichen Stellen und Körperschaften sowie Firmen abschließen.

Die Bedeutung dieser Kommission kann nicht hoch genug eingeschätzt werden, da sie die Voraussetzung bietet, aufgrund ihrer weitreichenden Befugnisse und der intimen Detailkenntnisse durch eine schrittweise Normfindung bereichsspezifische Datenschutzregelungen für die verschiedensten Gebiete herbeizuführen.

### 3. DATENBANKREGISTER

#### 3 Datenbankregister

In Hessen hat sich der Bestand der EDV-Anlagen und der EDV-Erfassungsstellen im Berichtszeitraum kaum verändert. Es wurden jedoch von der Verwaltung wesentlich mehr Aufgaben der Automation zugeführt. Das gilt vor allem für das Finanzwesen, das Einwohnerwesen und das Personalwesen.

verarbeitungs- und die Datenaufbewahrungsstellen (siehe Muster A).

Aus einem zweiten Teilregister ist zu ersehen, welche Stellen (Behörden) für welche Aufgaben welche Datenarten speichern. Zur besseren Übersicht erhalten die Stellen (Behörden) eine Hauptnummer und die einzelnen Aufgaben davon abgeleitete Unternummern (Aufgabennummern). Die Kommunalbehörden haben z. B. die Nr. 1, die von ihnen wahrzunehmenden Aufgaben: Einwohnerwesen die Nr. 101, der Nachweis der Arbeitsstätten Nr. 102 usw. (siehe Muster B).

#### 3.1 Datenartenkatalog

Um Art, Umfang und Auswirkungen der maschinellen Datenverarbeitung beobachten zu können, hat der Datenschutzbeauftragte einen Datenartenkatalog erstellt. Die Grundlage dazu waren die von den Ressorts vorgelegten Erfassungsbögen und Mitteilungen über Datenverarbeitung der Behörden des Landes und der der Aufsicht des Landes unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts. Dieser Datenartenkatalog dient:

dem Datenschutzbeauftragten als Arbeitsmittel und dem Bürger als Auskunftsregister.

Der Datenartenkatalog soll zu einem automatisierten Datenbankregister weiterentwickelt werden. Bereits der Datenartenkatalog besteht aus einem Verzeichnis der einzelnen Datenarten mit ihrer Zuordnung zu den automatisierten Aufgaben und den Stellen der öffentlichen Verwaltung. Das Verzeichnis enthält keine Individualangaben, sondern gibt dem Bürger Auskunft darüber, welche Stellen (Behörden) Daten speichern, wohin sie die Daten weitergeben und für welche Zwecke sie verwendet werden. Den Inhalt der über ihn gespeicherten Daten muß der Bürger bei den speichernden Stellen selbst erfragen.

Um dem Bürger Auskunft darüber zu geben, welche Stellen (Behörden) Daten über ihn gespeichert haben könnten, werden in einem Teilregister alle datenverarbeitenden Stellen erfaßt. Dieses Teilregister enthält Angaben über die Dienststelle, die Datenverarbeitungs-Aufgabe, ob personen- oder sachbezogen, die Datenermittlungs-, die Datenerfassungs-, die Daten-

#### Muster B: (Beispiel)

Welche Stelle speichert welche Datenarten?

		Aufgaben-Nummer			
		101	102	103	104
1 Kommunalbehörden					
Datenarten	Aufgaben	Einwohnerwesen mit Einwohner-, Lohnsteuer-, Wahl- und Impfdaten	Nachweis der Arbeitsstätten	Berechnung und Zahlbarmachung nach den Sozialgesetzen	Gemeindeabgaben und -steuern
	Name, Vorname, Titel		x	x	x
Wohnort		x		x	
Straße, Hausnummer		x		x	
Geburtsdatum		x		x	
Geburtsort		x		x	
usw.					

#### Muster A: (Beispiel)

Verzeichnis der datenverarbeitenden Dienststellen

Dienststelle	Aufgabe der Datenverarbeitung	Pers. oder Sachbez.	Datenermittlungsstelle	Datenerfassungsstelle	Datenverarbeitung	Aufbew. der Ergebnisse
Gemeinde A	Einwohnerwesen	P	Gemeinde	Landkreis	KGRZ	Gemeinde
Landkreis A	Techn. Berechnungen (Grundstücksvermessung usw.)	S	Katasteramt	Katasteramt	KGRZ	Katasteramt

Aus einem dritten Teilregister soll ersichtlich sein, wohin die Stellen (Behörden) die Daten gegebenenfalls bei der Aufgabendurchführung weitergeben; z. B. geben die Kommunalbehörden (1) Daten aus dem Einwohnerwesen (101) weiter an die Meldeämter, Polizeidienststellen, die Wehrerfassungsstellen, das Wahl- und das Gesundheitsamt (siehe Muster C).

**Muster C: (Beispiel)**

1 Kommunalbehörden:	Weitergabe der Daten an:
101 Einwohnerwesen (Einwohner-, Lohnsteuer-, Wahl- und Impfdaten)	Meldeämter Polizeidienststellen Wehrerfassungsstelle Wahlamt Gesundheitsamt

Das für den Bürger wichtigste Teilregister (Muster D) dürfte das „Verzeichnis der Datenarten“ sein, da er daraus erfahren kann, welche Stellen für welche Aufgaben z. B. die Berufs- oder die Familienstandsdaten gespeichert haben. Es ist z. Z. nach Anfangsbuchstaben geordnet und enthält rund 500 Angaben über die Datenarten und verweist auf rund 800 mögliche Nutzungen innerhalb des Aufgabenbereiches der einzelnen Dienststellen. Allein die Datenart „Namen“ wird z. B. für 40 verschiedene Verarbeitungen genutzt.

Beim „Beruf“ sind es drei und beim „Familienstand“ neun (siehe Muster D).

**Muster D: (Beispiel)**

Datenart	Aufgaben-Nummer
Alter Wohnsitz	1002
Altersversicherung	1001
Anschrift des Ehegatten	106
Beruf	601, 602, 604
Berufsfähigkeit des Ehegatten	106
Berufsziel	1003
Datum des Zuzugs	101, 102, 103
Daten der Fahrerlaubnis	301, 302
Familienstand	101, 102, 104, 106, 202, 1001, 1002, 1003, 1009
Familienstandsänderung	101, 102, 103
Geburtsort	101, 102, 104, 106, 301, 302, 509, 701, 801, 1003

Für den Ausbau des Datenartenkatalogs zu einem Datenbankregister sind folgende Voraussetzungen zu schaffen:

1. Datenartenverzeichnis
  - 1.1 Verzeichnis der gespeicherten Datenarten geordnet nach Anfangsbuchstabe mit Aufgaben-Nummer
  - 1.2 Nachweis über Mehrfachspeicherung von Datenarten mit zugehöriger Aufgaben-Nummer

2. Verzeichnis der datenverarbeitenden Dienststellen
  - 2.1 Dienststelle
  - 2.2 Aufgabe der Datenverarbeitung
  - 2.3 Datenverarbeitung personen- oder sachbezogen
  - 2.4 Datenermittlungsstelle
  - 2.5 Datenerfassungsstelle
  - 2.6 Datenverarbeitungsstelle
  - 2.7 Datenergebnissammelstelle
3. Bestandsnachweis (siehe Muster E)
  - 3.1 Nachweis aller Stellen, die Aufgaben durch EDV erledigen, nach Ressorts geordnet
  - 3.2 Aufgabe der Datenverarbeitung
  - 3.3 Verzeichnis der verarbeitenden Stellen mit Ortsangabe
4. Verknüpfungs- und Suchmerkmale
 

Die geplanten Dienststellennummern der Behörden, Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts werden als Verknüpfungs- und Suchmerkmale verwendet.
5. Nachweis der Aufgaben-Nummern
  - 5.1 Aufgaben-Nummer mit Angabe der Aufgabe der Datenverarbeitung
  - 5.2 Aufgaben-Nummer mit Nachweis der Datenweitergabe
6. Nachweis der gespeicherten Datenarten und Datengruppen
7. Maschinenkapazität
  - 7.1 Dienststellen-Nummer
  - 7.2 Bezeichnung der Anlage
  - 7.3 Speicherkapazität
  - 7.4 Peripheriegeräte
8. Verarbeitung bei Service-Unternehmen
  - 8.1 Verzeichnis der Stellen, die Service-Unternehmen in Anspruch nehmen, mit Angabe des Service-Unternehmens
9. Datenverarbeitung außer Haus
  - 9.1 Verzeichnis der Stellen, die bei anderen Stellen der öffentlichen Verwaltung Daten verarbeiten lassen
10. Verzeichnis der Verarbeitungs- und Auswertungsprogramme
11. Verzeichnis der periodisch ausgewerteten Dateien
12. Zeitverzeichnis für Programmläufe und Auswertungen

**Muster E: (Beispiel)****7.0 Der Hessische Minister für Wirtschaft und Technik****7.01 Straßenbauverwaltung****7.0101 Technische Berechnung  
(Straßendatenbank vorgesehen)****7.0102 Arbeiter-Lohnberechnungen****7.04 Industrie- und Handelskammern****7.0401 Berechnung der Kammerbeiträge und Überwachung der Berufsausbildung**

7.0400001 Darmstadt

7.0400002 Frankfurt/M.

7.0400003 Fulda

7.0400004 Gießen

7.0400005 Offenbach

**3.2 Protokollierung**

Die Protokollierung dient der internen Kontrolle der ordnungsmäßigen und programmgerechten Datenverarbeitung sowie der Statistik und Auswertung. Bei Datenfernverarbeitung ist jede Abweichung im Systemablauf sofort und sichtbar festzuhalten.

Jede Eröffnung eines Jobs (= Auftrag zur Eröffnung einer Programmfolge) sollte nach Uhrzeit, benutztem Programm, Benutzerberechtigung und Benutzeridentifikation automatisch protokolliert werden. Hat ein Teilnehmer eine Datei oder ein Programm unberechtigt angesprochen, hat ihn das System abzuweisen und automatisch den versuchten Einbruch ins System über das Konsolprotokoll anzuzeigen.

Die Protokollierung ist ein Mittel, nachträglich zu kontrollieren, welche Arbeitsvorgänge die Maschine geleistet hat. Aus dem Protokoll ist jedoch nicht mit Sicherheit zu entnehmen, ob das Verarbeitungsprogramm durch Manipulationen verändert worden ist oder Einstiegsmöglichkeiten für unzulässige Manipulationen gewährt. Um eine automatisierte Kontrolle über den ordnungsgemäßen Ablauf der Datenverarbeitung einführen zu können, müßte untersucht werden, ob man Kontroll- oder Analyseprogramme entwickeln könnte, mit denen Abweichungen oder andere Manipulationen automatisch festgestellt werden können. Diese Kontroll- oder Analyseprogramme müßten parallel mit dem Verarbeitungsprogramm laufen und sollten nach Möglichkeit den Ablauf des Programms stoppen, wenn Abweichungen festgestellt werden.

In den Vereinigten Staaten hat die amerikanische IBM bereits eine umfangreiche Untersuchung über derartige Datensicherungsmöglichkeiten durchgeführt. In einer ersten Fühlungnahme mit einem Institut der Technischen Hochschule Darmstadt ist festgestellt worden, daß dort die Bereitschaft besteht, dieses Problem wissenschaftlich zu untersuchen und Grundlagen für eine technische Verwirklichung zu erarbeiten. Dieses Problem ist im Dritten Tätigkeitsbericht (vgl. 4.3.3) bereits aufgezeigt worden.

Solche Untersuchungen wären für die Fortentwicklung des Datenschutzes von großer Bedeutung. Sie würden die Sicherheit der Datenverarbeitung außerordentlich vergrößern.

Deshalb wird angeregt, die notwendigen Mittel für derartige Forschungsaufträge an einer geeigneten Haushaltsstelle zur Verfügung zu stellen.



## 4. TÄTIGKEITEN DES DATENSCHUTZBEAUFTRAGTEN

### 4 Tätigkeiten des Datenschutzbeauftragten

Die Tätigkeit des Datenschutzbeauftragten hat sich im Berichtszeitraum ausgeweitet. Vermehrt wurde er — wie bereits ausgeführt — aufgefordert, an Beratungen, Diskussionen, Anhörungen und Interviews auf bundesdeutscher und internationaler Ebene teilzunehmen. Auch die Zahl der schriftlich und mündlich eingegangenen Beschwerden hat sich erhöht; über die Konsequenzen, die sich aus den daraufhin erfolgten Nachprüfungen ergaben, wird unter 4.4ff. berichtet.

#### 4.1 Präventives Wirken

Die Stellungnahmen der Landesregierung ziehen aus den bisher vorgelegten Tätigkeitsberichten des Datenschutzbeauftragten den Schluß, es bestehe kein Anlaß zu der Besorgnis, daß gegenwärtig von der öffentlichen Verwaltung in der EDV die Grundsätze des Datenschutzes mißachtet werden. Soweit der Datenschutzbeauftragte einzelne Fälle eines Mißbrauchs der EDV aufzeigt, will die Landesregierung diesen Rügen nachgehen. Diese Fälle sind jedoch nur Beispiele für mögliche Entwicklungstendenzen.

Nach der Anlage des Datenschutzgesetzes und nach dem Inhalt, den der Datenschutzbeauftragte dieser Rechtsvorschrift durch seine Tätigkeit gegeben hat, liegt der Schwerpunkt seines Auftrages weniger in der Kontrolle der einzelnen datenverarbeitenden Verwaltungsstellen — dies ist Sache der Aufsichtsbehörden. Er überwacht vielmehr in erster Linie die sich anbahnenden Entwicklungen und Trends und beurteilt ihre Bedeutung für die Selbstbehauptung des Individuums gegenüber einer immer stärker mechanisierten Verwaltungsapparatur sowie die Rückwirkungen solcher Entwicklungen auf das Verhältnis von Parlament und Regierung. Nach seinem Selbstverständnis bedeutet Datenschutz Besorgnis in Permanenz.

Auf anderen Gebieten erleben wir immer aufs Neue, daß gegenüber der angestrebten Steigerung der Rationalität und Effektivität von Verfahren und Einrichtungen kritische Erwägungen darüber, ob die individuelle Selbstbestimmung dadurch beeinträchtigt und allgemeine humanitäre Bestrebungen gefährdet werden könnten, nicht ausreichend oder erst dann berücksichtigt werden, wenn ein Schaden schon eingetreten ist. „Daten-Müll“ soll es in Hessen nicht geben. Dies soll nach Möglichkeit verhindert werden. Das präventive Wirken des Datenschutzbeauftragten hat Vorrang vor nachträglicher Kontrolle. In dieser Beurteilung stimmt die Landesregierung mit dem Datenschutzbeauftragten überein und unterstützt seine Bemühungen.

#### 4.2 Datenschutz in Rechenzentren

Besonders beachtet hat der Datenschutzbeauftragte im Berichtszeitraum die Entwicklung innerhalb des

hessischen Datenverarbeitungs-Verbundes [die Hessische Zentrale für Datenverarbeitung (HZD) und die fünf regionalen Kommunalen Rechenzentren (KGRZ)]. Obwohl die gemeinsamen Datenschutz-Richtlinien zur Gewährleistung des Datenschutzes und der Datensicherheit im DV-Verbund (DASCH) noch immer in der Erprobung sind, werden die darin enthaltenen Vorschriften im allgemeinen von den Rechenzentren berücksichtigt. Der Datenschutzbeauftragte konnte sich bei verschiedenen Besuchen davon überzeugen, daß die getroffenen Maßnahmen zwar nicht einheitlich sind, weil die unterschiedlichen örtlichen Gegebenheiten berücksichtigt werden, daß aber in fast allen Fällen die notwendigen Vorkehrungen getroffen worden sind. Das gilt sowohl für

- die Trennung der einzelnen Verarbeitungsfunktionen;
- den closed-shop-Betrieb, insbesondere die strenge Trennung von Programmierung und maschineller Datenverarbeitung. Zu dem Computerraum erhalten durch optische und akustische Kontrollen nur befugte Mitarbeiter Zutritt;
- die räumliche und funktionelle Trennung des Datenträger-Archivs vom Maschinensaal;
- den Grundsatz, daß Datenträger nur für den aktuellen Arbeitsvorgang an das Bedienungspersonal ausgegeben werden und nach Beendigung der Arbeit sofort zurückgehen;
- die Anordnung, daß keine leeren Arbeitsbänder im Maschinensaal herumliegen;
- das Sicherheitsschloß-System auf elektronischer Basis und die Regelung der Schlüsselvergabe;
- den Grundsatz, daß der Maschinensaal nicht von außen einsehbar sein soll;
- die Ausrüstung der Fenster mit bruchsicherem Glas, mit Alarmanlage und mit Stahlrahmen und der Türen mit Öffnungsmeldern, die auf unbefugtes Öffnen und Glasbruch ansprechen und
- den Anschluß an eine Alarmanlage.

In Rechenzentren, in denen diese Maßnahmen beim Aufbau noch nicht berücksichtigt worden waren, wurden sie inzwischen zumindest teilweise nachgeholt oder soll dies in Kürze geschehen.

Es gibt jedoch Rechenzentren, in denen die Datensicherungsmaßnahmen nicht ausreichen, weil die entsprechenden Vorschriften beim Bau noch nicht bekannt waren. Dem nachträglichen Einbau der notwendigsten Sicherungsmaßnahmen sollte nicht mit dem Argument begegnet werden, er erfordere Gelder, die dann bei der Beschaffung neuer Maschinen fehlten. Das würde nur beweisen, daß die EDV-Verwaltung der Effektivität in der Prioritätsskala einen wesentlich höheren Rang zuweist als dem Datenschutz,

der nur als lästiges Anhängsel betrachtet wird. Auch sind kurzfristig organisatorische Maßnahmen — wie z. B. der closed-shop-Betrieb — möglich, die praktisch keine Mehrausgaben erfordern.

In der ersten Aufbauphase war es noch verständlich — wenn auch nicht ohne weiteres entschuldbar — daß zuerst daran gedacht wurde, die Datenverarbeitung in Gang zu setzen. Aus räumlichen, organisatorischen und personellen Gründen traten Datenschutz und Datensicherung in den Hintergrund. Diese Phase ist aber beendet. Die in DASCH vorgeschriebenen organisatorischen Maßnahmen müssen in allen Rechenzentren durchgeführt und die technischen und baulichen Veränderungen baldmöglichst in Angriff genommen werden. Wie notwendig dabei die Anlegung eines strengen Maßstabes ist, beweist die Tatsache, daß eine der kürzlich unter dem Verdacht der Ostspionage verhafteten Personen einige Monate als Wartungstechniker des Computer-Herstellers in einem Rechenzentrum des Verbundes gearbeitet hat.

Der Datenschutzbeauftragte hat den Ministerpräsidenten von seinen Feststellungen unterrichtet und gebeten, auf die zuständigen Stellen entsprechend einzuwirken.

#### 4.3 Mitarbeit in Verwaltungsausschüssen

Um zu untersuchen, welche Aufgaben der Landesverwaltung oder der Gemeinden und Landkreise durch die EDV erledigt werden, und welchen Prioritätsrang sie erhalten sollen, wurden seinerzeit für die beiden Bereiche je ein Arbeitsausschuß für die Automation von Verwaltungsaufgaben gebildet. An den Sitzungen beider Ausschüsse kann der Datenschutzbeauftragte als Beobachter teilnehmen.

Die Mitarbeit in den beiden Ausschüssen hat jedoch gewisse Probleme aufgeworfen und bei manchen Stellen zu der Auffassung geführt, der Datenschutzbeauftragte sei Teil der Verwaltung und habe bei den der EDV zugeführten Verwaltungsaufgaben die Verantwortung für den Datenschutz zu übernehmen. Der Datenschutzbeauftragte hat jedoch keine Exekutivkompetenz. Die Verwaltungsbehörden sind nach wie vor für die Durchführung der Datenschutzmaßnahmen verantwortlich. Die Teilnahme des Datenschutzbeauftragten an Sitzungen der Ausschüsse — z. T. auch von Unterausschüssen und Arbeitsgruppen — und die Vorlage aller Protokolle dienen lediglich zu seiner Information über die Entwicklung der Datenverarbeitung in der öffentlichen Verwaltung, zur Prüfung der sich dabei möglicherweise ergebenden Gefahren sowie zur Beobachtung der Auswirkungen auf die Arbeitsweise und die Entscheidungsbefugnisse der Behörden. Gleichzeitig gibt ihm diese Teilnahme und ständige Information die Möglichkeit, bei den datenverarbeitenden Behörden Maßnahmen zur Verbesserung des Datenschutzes anzuregen. Es liegt jedoch im Ermessen und in der Verantwortung der Verwaltung, ob und in welcher Form sie diese Anregungen aufgreift und realisiert. Obwohl der Datenschutzbeauftragte in den beiden Ausschüssen kein Stimmrecht hat und aufgrund seiner Stellung außerhalb der Verwal-

tung auch nicht haben kann, sind seine Anregungen stets eingehend diskutiert und im allgemeinen auch entsprechende Regelungen gesucht worden.

Um bereits bei der Entwicklung von Datenverarbeitungsverfahren eine umfassende und einheitliche Untersuchung und Lösung der Datenschutzfragen zu ermöglichen, hatte der Datenschutzbeauftragte z. B. dem Ausschuß (Land) vorgeschlagen, bestimmte Datenschutzvorschriften in die gemeinsamen Richtlinien für die Automation von Aufgaben der Landes- und Kommunalverwaltung aufzunehmen. Nach einer umfassenden Diskussion hat der Ausschuß beschlossen, daß in den Abschlußberichten der Verfahrensentwicklung anzugeben sind

- die vorgesehenen Datenschutzmaßnahmen,
- die Rechtsvorschriften, aufgrund derer die Behörde Daten für das automatische Verfahren erhält,
- eine Stellungnahme über die Zulässigkeit der Vergabe der Datenerfassung an private Service-Unternehmen, sofern die Vergabe beabsichtigt ist, und
- Mindest- und Höchstaufbewahrungsfristen für die Daten, Programme und Programmdokumentationen.

Wie notwendig hier eindeutige Vorschriften für den Verfahrensablauf sind, ergibt sich aus den während der Ausschusssitzungen getroffenen Feststellungen, daß immer wieder Verwaltungen sich über die bereits heute geltenden Richtlinien hinwegsetzen und Verfahrenstests durchführen, bevor sie den Abschlußbericht vorgelegt haben.

#### 4.4 Datenfernverarbeitung im Einwohnermeldewesen

Im Berichtszeitraum hat der Automationsausschuß der Gemeinden und Landkreise die Grundstufe Einwohnerwesen für die EDV freigegeben. Inzwischen wurde auch bei einer der zuständigen Behörden die erste Stufe eines kommunalen Datenfernverarbeitungssystems des Einwohnermeldewesens Hessens in Betrieb genommen. Bei der Eröffnung nannte der Ministerpräsident die Anlage einen wichtigen Schritt auf dem Weg zu der von der Landesregierung 1969 entwickelten Konzeption einer integrierten Datenverarbeitung im Bereich der öffentlichen Verwaltung. Die Automatisierung des Einwohnerwesens solle die Integrationsbasis eines für alle kommunalen Einrichtungen und das Land offenen Informationssystems abgeben.

In einem Bericht über die Eröffnung heißt es, „besonderes Interesse fand bei den zahlreichen Gästen die praktische Demonstration des Datenschutzes“. Bei einer Besichtigung der Terminal-Station mußte der Datenschutzbeauftragte jedoch feststellen, daß die getroffenen Sicherheitsmaßnahmen nicht ausreichen. So erschien das Codewort bei der Abfrage auf dem Bildschirm des Terminals. Der Versuch, Daten einer anderen Gemeinde abzurufen, wurde zwar vom System mit dem Hinweis abgewiesen, daß die Abfrage unberechtigt erfolgt sei. Bei der Nachfrage in dem Kommunalen Gebietsrechenzentrum, das die Einwohnerdatei verarbeitet, wurde aber festgestellt, daß die Abweisung nicht — wie erforderlich — protokolliert wor-

den war. Die zuständige Stelle ist auf diesen Programmfehler aufmerksam gemacht worden.

Bei der Besichtigung dieser Terminal-Station erhielt der Datenschutzbeauftragte auch die Auskunft, daß die standesamtlichen Veränderungsdaten an beide christliche Kirchen im Original zur Einsicht weitergegeben werden. Die Praxis dieser Behörde dürfte kein Einzelfall sein.

#### 4.5 Informationssysteme bei Verfassungsschutz und Polizei

Die in den früheren Tätigkeitsberichten als notwendig bezeichnete Verrechtlichung der Weitergabe von Daten aus dem Informationssystem des Verfassungsschutzes (NADIS) an außerhalb des Systems stehende Behörden (z. B. zur Überprüfung von Personen, die an sicherheitsempfindlichen Stellen beschäftigt werden — Verfassungsschutzgesetz des Bundes i. d. F. vom 7. 8. 1972 — BGBl. 72/I, S. 1382) (vgl. III, 4.1.5.2) ist bisher nicht erfolgt. Die Landesregierung begründet dies in ihrer Stellungnahme (LT-Drucksache 7/5597/13) damit, daß es unmöglich sei, in einem Gesetzeskatalog einzeln aufzuführen, unter welchen Voraussetzungen Auskünfte von dem Landesamt verlangt werden können. Dies hat der Datenschutzbeauftragte auch nicht gefordert. Es geht ihm vielmehr um die rechtliche Fixierung des Verfahrens zur Festlegung der Personen und Stellen, die auskunftsberechtigt sind. Vergleichbar wäre die Regelung der Auskunftsberechtigung im Bundeszentralregister. Diese Frage könnte durch Landesgesetz geregelt werden, während dagegen die Zusammenarbeit des Landesverfassungsschutzamtes mit den anderen Verfassungsschutzämtern bundeseinheitlich geregelt sein muß.

Grundsätzlich das gleiche gilt für das polizeiliche Informationssystem in Hessen, HEPOLIS, das Teil des bundesweiten polizeilichen Informationssystems INPOL ist. Der Datenschutzbeauftragte hatte in den vergangenen Berichten angeregt, die Regelung der Verwendung und Weitergabe personenbezogener Daten durch die Polizei zu verrechtlichen. Die Landesregierung und das Hessische Landeskriminalamt haben dazu erklärt, daß eine solche Regelung aus rechtlichen Gründen nicht auf Landesebene beschränkt bleiben könne.

Es wird aber dabei verkannt, daß es sich bei den Forderungen des Datenschutzbeauftragten um zwei verschiedene Fragen handelt. Soweit es darum geht, an welche Stellen, z. B. an die Aufsichtsbehörde oder an andere hessische Landesbehörden, die nicht Polizeibehörden sind, die Polizei Informationen aus ihrem System herausgeben darf, und welche Auflagen diesen Behörden für die Aufbewahrung und Verwertung dieser Information zu machen sind, handelt es sich um eine innerhessische Angelegenheit. Sie kann daher durch Rechtsverordnung oder durch Landesgesetz geregelt werden.

##### 4.5.1 Zusammenarbeit mit anderen Ländern und Bund

Die Zusammenarbeit der Polizeien der Länder und des Bundes bedarf dagegen einer bundeseinheitlichen

Regelung. Hier hatte der Datenschutzbeauftragte vorgeschlagen, die hessischen Erfahrungen als Anregungen in die Diskussion auf Bundesebene einzubringen. Das Hessische Landeskriminalamt hat diese Anregung aufgegriffen. Nach Umfragen beim Bundeskriminalamt sowie allen anderen Landeskriminalämtern hat es vorgeschlagen, die Richtlinien über die Führung von Kriminalakten zu überarbeiten und einen neuen, bundeseinheitlichen Richtlinienentwurf vorzulegen. Die Arbeitsgemeinschaft der Leiter der Landeskriminalämter mit dem Bundeskriminalamt (AG-Kri-po) faßte daraufhin im Juni 1974 den Beschluß, unter Federführung des Landes Hessen eine Fachkommission zu bilden, „die sich unter Anlehnung an das Gesetz über das Zentralregister und das Erziehungsregister (BZRG) vom 18. 3. 1971 mit der Überarbeitung der Richtlinien für die Führung von Kriminalakten befaßt und dabei auch die Erfordernisse des Datenschutzes berücksichtigt“. Diese Fachkommission hat den Entwurf einer Polizeidienstvorschrift über die Führung von Kriminalakten erarbeitet. Sie wird jetzt der Innenminister-Konferenz vorgelegt.

Der Inhalt derartiger Entwürfe sollte bereits im Stadium der Vorbereitung öffentlich diskutiert werden. Da sich hier mehrere zuständige Stellen (Landesregierungen und Bundesregierung) auf gemeinsame Grundlinien verständigen müssen, ist es — wie die Erfahrung zeigt — im allgemeinen schwierig, nachträglich noch Veränderungen der einmal gefundenen Lösung herbeizuführen. Es bleibt dann gewöhnlich nur der Ausweg, bereits beschlossene Regelungen ohne Änderung zu akzeptieren oder in der Gesamtheit abzulehnen.

Es mag zutreffen, daß eine absolute Verrechtlichung des Umgangs mit Polizeinformationen (hier gemeint als Gesetze, Rechtsverordnungen oder als Selbstbindung an vorher veröffentlichte Regeln) nicht immer zweckmäßig ist. Zweifellos darf die Verbrechensbekämpfung nicht durch mangelnde Elastizität erschwert werden. Um so notwendiger ist die Abgrenzung der Kompetenzen und die Festlegung der Verantwortlichkeiten, denn zweifellos hat die EDV die Situation auch bei der polizeilichen Informationsverarbeitung verändert.

Es geht in erster Linie darum, die unbefugte Anwendung regelrechter Schleppnetz-Techniken unmöglich zu machen und zu verhindern, daß Informationen über Personen, die mit bestimmten Straftaten in Verbindung gebracht werden, ohne daß die Angaben beweisbar sind, Unbefugten oder der Öffentlichkeit zugänglich gemacht werden können. Auch für die Innenminister müssen die Verantwortlichkeiten festgelegt sein, denn immerhin gibt es — mit den 11 Ländern und dem Bund — 12 Innenminister bzw. -Senatoren. Daß auch diese „Spitzen“ gebunden sein müssen, zeigt der Umgang des rheinland-pfälzischen Innenministers Schwarz mit polizeilichen Erkenntnissen, die außerhalb seines Landes gewonnen worden waren: Er hat dabei Unterlagen der Öffentlichkeit unterbreitet, die auch unbewiesene Angaben über Personen außerhalb seines Amtsbereichs enthielten, die nicht wegen anderer bewiesener oder nachweisbarer Straftaten verfolgt werden.

Ebenso ist sicherzustellen, daß die Regelungen des Bundeszentralregistergesetzes (früher Strafregister) nicht beliebig unterlaufen werden können. Da jeder Polizeibeamte die Möglichkeit hat, aus dem polizeilichen Informationssystem Auskünfte abzufragen, müssen diese Auskünfte protokolliert werden, um jederzeit nachprüfen zu können, daß er sie im Zusammenhang mit einer dienstlichen Aufgabe benötigt hat. Es muß ausgeschlossen sein, daß er das Informationssystem für private Zwecke mißbraucht, evtl. um festzustellen, ob gegen seinen Nachbarn, mit dem er im Streit liegt, oder gegen den neuen Freund seiner Freundin polizeiliche Erkenntnisse bzw. ein Verdacht wegen strafbarer Handlungen vorliegen. Warnendes Beispiel ist der Versuch des ehemaligen US-Präsidenten Nixon, durch systematische Nachforschungen bei der Steuerfahndung, beim Rauschgiftdezernat oder allgemein in Unterlagen der Verbrechensbekämpfung belastende Angaben über politische Gegner zu sammeln.

Um diesen Gefahren zu begegnen, wird in den USA in zunehmendem Maß sowohl auf nationaler als auch auf einzelstaatlicher Ebene die Lösung dieses Problems diskutiert und z. T. bereits realisiert. Die ständige Überprüfung der Weiterentwicklung der Informationssysteme und der Praktiken im Umgang mit Polizeiinformationen wird sachverständigen Beratungsorganen (Beiräten) übertragen, in denen außer Polizeifachleuten auch Politiker, Publizisten, Richter, Vertreter von Kirchen, Gewerkschaften etc. mitwirken.

#### 4.5.2 Regelung in HEPOLIS

Die hessische Vollzugspolizei hat nach Einführung der EDV umfangreiche Maßnahmen zur Gewährleistung des Datenschutzes in ihrem Informationssystem HEPOLIS getroffen. Dabei hat sie die Datenschutz-Richtlinien (DASCH), soweit sie für sie anwendbar waren, berücksichtigt. Aus Darlegungen der Polizei ist zu entnehmen, daß Sicherheitsvorkehrungen getroffen sind, die verhindern, daß Bedienstete das Informationssystem für private Zwecke mißbrauchen können. Ein Sicherheitsbeauftragter des Landeskriminalamtes sorgt für die Einhaltung der Datenschutz- und Datensicherungsvorschriften.

#### 4.6 Weitergabe von Einzelangaben aus Bundesstatistiken

Eine vom Statistischen Landesamt in zwei Fällen geleistete bzw. beabsichtigte Amtshilfe hat zu einer grundsätzlichen Meinungsverschiedenheit über die Befugnis des Statistischen Landesamtes geführt, personenbezogene Daten, die für eine Bundesstatistik erfaßt worden sind, an andere Behörden offen, d. h. mit Namen und Anschrift weiterzugeben.

Nach Auffassung des Statistischen Landesamtes entfällt die Geheimhaltungspflicht, wenn es sich um eine „allgemein bekannte Tatsache“ handelt oder wenn der Betroffene auf den Geheimhaltungsschutz ausdrücklich verzichtet. Das Statistische Landesamt beauftragt dabei auf „Empfehlungen zur Auslegung des geltenden Rechts in Fragen der Geheimhaltung“, die der Rechtsauschuß der Statistischen Landesämter am 27. 5. 1963 zusammengestellt hat.

Hierzu ist folgendes zu bemerken:

Die vorgenannten Empfehlungen des Rechtsausschusses der Statistischen Landesämter stammen aus einer Zeit, als die spezifischen Gefahren der maschinellen Datenverarbeitung für das Persönlichkeitsrecht noch nicht aktuell waren und daher nicht berücksichtigt wurden. Heute ist es dagegen in der Rechtsprechung und in der Wissenschaft anerkannt, daß die Befugnis, behördlich gesammelte Daten weiterzugeben, nach den Erfordernissen des Persönlichkeitsrechts zu beurteilen ist. Dies gilt vor allem, wenn die Daten einem besonderen Berufs- oder Amtsgeheimnis unterliegen. Die Geheimhaltung statistischer Daten und die Amtshilfe ist für die Statistischen Ämter in § 12 Abs. 1 und Abs. 2 StatGes geregelt. Die extensive Auslegung dieser Vorschriften ist angesichts der neuesten Entwicklung der Datenverarbeitung nicht mehr zulässig. Die juristischen Einzelheiten der Meinungsverschiedenheit sollen an dieser Stelle nicht erörtert werden. Jedoch erscheint es geboten, die aus dem Jahr 1963 stammenden „Empfehlungen zur Auslegung des geltenden Rechts in Fragen der Geheimhaltung“ zu überprüfen.

#### 4.7 Datenschutz in Individualdateien und bei Sondererhebungen

Zahlreiche Befragungsaktionen (vgl. unter 1.2) finden im Schul- und Hochschulbereich für Forschungszwecke der Pädagogik und der Psychologie statt; sie werden aber auch für andere amtliche und private Planungen durchgeführt. Die Einhaltung der Grundregeln der Datenverkehrs-Ordnung wäre dabei jedoch die unabdingbare Voraussetzung zur Erhaltung des Persönlichkeitsrechts. Das gilt besonders auch dann, wenn wissenschaftliche Institute oder private Unternehmen mit der Durchführung der Befragung betraut werden.

##### 4.7.1 Schulsportärztlicher Untersuchungsbogen

Welche Maßnahmen die Datenverkehrs-Ordnung (vgl. Anlage I) in der Praxis erforderlich macht, zeigt das bereits im Dritten Tätigkeitsbericht (III, 4.1.1.3, S. 27) erwähnte Projekt „schulsportärztlicher Untersuchungsbogen“. Auf einem „Erfassungsblatt“ des Sportlers für den Sportarzt werden eine Reihe von Daten erfaßt, die der Sportler meist nur seinem Arzt und vielleicht seinen nächsten Angehörigen mitteilt, die er aber vor jedem anderen verheimlichen würde. Die Angaben sind aber erforderlich, weil ohne sie der Sportarzt weder die Sporttauglichkeit beurteilen noch den Sportler über die Art und Intensität seines Trainings beraten könnte. Den Anforderungen des Datenschutzes wurde bei dem Projekt „schulsportärztlicher Untersuchungsbogen“ durch die von Anfang an bestehende Zusammenarbeit des federführenden Sozialministeriums mit dem Datenschutzbeauftragten zunächst entsprochen.

##### 4.7.2 Gesundheitsdatenbanken

Das Projekt „schulsportärztlicher Untersuchungsbogen“ ist als erstes Teilstück des für später geplanten „Gesundheits-Informationssystems“ gedacht. Es soll

das lückenlose „Gesundheitsprofil“ eines Jugendlichen enthalten, das sich aus der Neugeborenenuntersuchung, Kleinkinderuntersuchung, schulärztlichen Untersuchung, schulspportärztlichen Untersuchung und Jugendarbeitsschutzuntersuchung ergibt und dann aus seiner „Jugendgesundheitskarte“ ablesen läßt. Diese Gesundheitskarte würde nach der Schulentlassung fortgeführt und könnte auch die Daten des Impfwesens, des Gesundheitsamtes, der stationären Behandlung im Krankenhaus und der ambulanten ärztlichen Behandlungen aufnehmen.

Unter Datenschutz-Gesichtspunkten wäre es bedenklich, wenn einzelne Projekte aus dem Bereich der medizinischen Datenverarbeitung verwirklicht werden, ohne daß konkrete Vorstellungen über die vorgesehene Integration in ein Gesundheitsinformationssystem öffentlich diskutiert worden sind. Hier würde „ohne Bebauungsplan“ gebaut, d. h. durch die Verwirklichung von Einzelprojekten ohne Vorliegen einer Gesamtkonzeption würden Tatbestände geschaffen, die bei einer möglichen späteren Zusammenführung medizinischer Datenbanken im Wege der Datenfernverarbeitung die Kontrolle des Datenschutzes erschweren, wenn nicht gar unmöglich machen. Über wesentliche Elemente derartiger Systeme, wie z. B. zentrale oder dezentrale Speicherung, die Zuständigkeiten und Kontrollen, die Weitergabe- und Zugriffsregelungen, die Anonymisierung, die Lösungsfristen und die Einsichtsrechte des Bürgers muß Klarheit bestehen.

#### 4.7.3 Schülerindividualdateien

Ein Beispiel für die mangelnde Beachtung der Grundsätze der Datenverkehrs-Ordnung ergibt sich aus den Projekten der Schüler- und Studentendateien. Mit Hilfe dieser Dateien soll die Beanspruchung pädagogischer Mitarbeiter durch Verwaltungsaufgaben reduziert und der Umfang der Verwaltungsarbeiten eingeschränkt werden.

Die notwendige parallele Entwicklung von Datenschutzvorstellungen und -maßnahmen bereits in der Konzeptionsphase eines neuen EDV-Projekts würde im Falle des Projekts „Schülerindividualdatei“ erforderlich machen, daß zunächst die wesentlichen Merkmale des geplanten „Schulinformationssystems“ (Aufgabenuntersuchung/Vorbericht zur Schülerindividualdatei) bekanntgegeben sowie Ziel und Zweck des Teilprojekts „Schülerindividualdatei“ innerhalb des Gesamtsystems verdeutlicht werden.

Es erscheint angebracht, in diesem Zusammenhang auf Entwicklungen in den USA aufmerksam zu machen, wo das Ende 1974 in Kraft getretene Gesetz über Elternrecht und Datenschutz (Family Educational Rights and Privacy Act of 1974) mit seinem sogenannten „Buckley Amendment“ (einer von Senator Buckley eingebrachten Ergänzung) folgendes festgelegt: Eltern haben das Recht, alle Akten und Dateien mit Angaben über ihre Kinder einzusehen und unrichtige oder ungenaue Daten korrigieren zu lassen. Sie müssen im übrigen um eine schriftliche Genehmigung gebeten werden, bevor Schulen Personendaten über ihre Kinder an dritte Stellen weitergeben dürfen.

#### 4.7.4 Studentendateien

Gleichartige Probleme stellen sich bei „Studentendateien“, d. h. Dateien mit personenbezogenen Daten von Studenten an Universitäten, Fachhochschulen und bei der Zentralstelle für die Vergabe von Studienplätzen (ZVS).

In einer Eingabe wurde der Datenschutzbeauftragte davon unterrichtet, daß vor dem Studiumabschluß stehende Studenten einer Hochschule von einem „Bauftragten der Organisation für Führungs- und Nachwuchskräfte“ besucht wurde. Es handelte sich in Wirklichkeit um den Vertreter eines Versicherungsunternehmens, der alle vor dem Studiumabschluß stehenden Studenten mit Name, Anschrift, Geburtsdatum und Fachbereich auf Karteikarten erfaßt hatte. Obwohl der Präsident der Hochschule bereits vor längerer Zeit die Weitergabe von Studentenadressen an Stellen außerhalb der Hochschulverwaltung untersagt hatte, konnte nicht festgestellt werden, woher der Vertreter die Adressen erhalten hat.

Es wäre wünschenswert, wenn die Aufsichtsbehörde Muster-Richtlinien erarbeiten würde, die gewährleisten, daß bei allen Hochschulen des Landes ein ausreichender Datenschutz für die personenbezogenen Daten der Studenten erreicht wird.

#### 4.7.5 Forschungstests an Schulen

Bei den eingangs geschilderten Befragungsaktionen für Forschungszwecke an hessischen Schulen (vgl. unter 1.2) wurden im allgemeinen — aber nicht in allen Fällen — die Leitung und der Elternbeirat der betreffenden Schulen unterrichtet, nicht aber die Eltern der befragten Schüler. Da Datenschutz aber ein Aspekt des grundrechtsgeschützten Persönlichkeitsrechts ist, kann die Zustimmung des Betroffenen nicht durch ein Repräsentativorgan — wie den Elternbeirat — ersetzt werden.

Werden Kinder in der Schule befragt, so sind neben den Interessen der Forschung und den Persönlichkeitsrechten der Kinder auch die der Eltern — vor allem, wenn sie in die Befragung mit einbezogen sind — und deren Erziehungsrecht (Art. 55 HV; Art. 6 GG) zu beachten.

Aus der Schulpflicht ergibt sich nicht die Pflicht zur Teilnahme an wissenschaftlichen Testuntersuchungen. Es ist auch nicht primäre Aufgabe der Schule, die Schüler für Forschungszwecke bereitzustellen. Die Freiwilligkeit der Teilnahme an solchen Tests ist daher unverzichtbar.

Wissenschaft und Forschung sind frei. Diese Befragungen und Tests mögen oft unentbehrliche Mittel für Planungsiniciativen und Gesetzgebungsvorhaben sein. Es ist Aufgabe der Verwaltung bzw. der obersten Schulaufsichtsbehörde, die wissenschaftliche Zuverlässigkeit und die rechtliche Zulässigkeit derartiger Testbefragungen zu beurteilen. Sie muß dabei die Persönlichkeitsrechte berücksichtigen.

#### 4.7.6 Unterrichtung des Datenschutzbeauftragten

Nach § 13 DSG sind „dem Datenschutzbeauftragten die ihm für die Erfüllung seiner Aufgaben notwendige“

gen Auskünfte zu erteilen“. Ferner hat das Kabinett mit Beschluß vom 7. Okt. 1970 angeordnet, „die einzelnen Behörden, Körperschaften, Anstalten und Stiftungen, auf die sich das Datenschutzgesetz erstreckt, anzuweisen, dem Datenschutzbeauftragten die Muster der Erfassungsbögen und andere Datenträger, aus denen sich ergibt, welche Daten oder Merkmale gesammelt werden, unverzüglich vorzulegen“.

Viele Stellen der öffentlichen Verwaltung sind der Auffassung, daß es sich dabei um eine einmalige Meldung gehandelt hat und nicht um eine laufende Verpflichtung. Es erscheint notwendig, alle Behörden darauf hinzuweisen, daß der Datenschutzbeauftragte von allen Vorhaben der Verwaltung — oder bei denen die Verwaltung beteiligt ist — unterrichtet wird, wenn sie mit Hilfe der EDV durchgeführt werden.

#### 4.7.7 Umgang mit Individualdaten

Auch eher abgelegene Gebiete, wie das Bibliothekswesen, treten neuerdings in den Mittelpunkt des Datenschutzinteresses. Ohne Zweifel sind für den Aufbau von Bibliotheken und die Anschaffung neuer Literatur das Verhalten und die Wünsche der Leser von großem Interesse, wenn Fehlinvestitionen vermieden werden sollen. Das gilt nicht zuletzt auch für Schulbibliotheken. Mit Unterstützung des Bundes wird deshalb an einer hessischen Schule ein Modell entwickelt, das dem Aufbau und Ausbau von Schulbibliotheken dienen soll. Dabei werden die persönlichen Daten jedes Bibliothekbenutzers erfaßt und das Leseverhalten des einzelnen Schülers untersucht. Obwohl dieses Eindringen in die Privatsphäre des Schülers nicht unproblematisch ist, enthielt die Projektbeschreibung zunächst keine Datenschutzmaßnahmen. Sie wurden erst auf Anregung des Datenschutzbeauftragten vorgesehen. Die zuständige Behörde war sich weder der Notwendigkeit von Datenschutzmaßnahmen bewußt, noch war ihr die Institution des Datenschutzbeauftragten bekannt.

Obwohl im Berichtszeitraum festgestellt werden kann, daß bei den öffentlichen Behörden das Datenschutzbewußtsein zugenommen hat, ist der geschilderte Vorgang kein Einzelfall. So hatte z. B. das Kultusministerium keine Bedenken, die Datei einer bestimmten Personengruppe mit Namensangabe und Informationen über den sozialen Status des einzelnen zur Verarbeitung einer Privatfirma zu überlassen, obwohl das Rechenzentrum sich bereiterklärt hatte, das Datenfeld mit Namen und Adresse unkenntlich zu machen. Die Anfrage des Datenschutzbeauftragten, weshalb die Anonymisierung nicht erfolgt und was mit den Daten nach der Auswertung durch die betreffende Firma geschehen sei, ist jetzt mit dem unzulänglichen Nachweis beantwortet worden, daß in diesem Fall die Daten nicht mißbraucht worden seien.

In einem anderen Fall verwandte ein Rechenzentrum für einen Testlauf personenbezogene Originaldaten. Die Informationsunterlagen über diesen Test wurden an zahlreiche Stellen weitergeleitet. Keiner dieser Stellen fiel auf, daß hier unzulässigerweise mit echten Daten gearbeitet wurde. Erst als der Datenschutzbeauf-

tragte den Fall aufgriff, wurde der Fehler erkannt und zugesichert, die Datenschutzvorschriften bei Testläufen in Zukunft zu beachten.

#### 4.7.8 Datenweitergabe für gewerbliche Zwecke

In vielen Fällen wird das Recht des Bürgers, selbst darüber zu bestimmen, was mit den von ihm gegebenen Daten geschieht, nicht oder doch nicht ausreichend beachtet. So enthält z. B. § 104 Abs. 1 der von der Bundesregierung erlassenen allgemeinen Verwaltungsvorschrift zum Personenstandsgesetz (Dienstausweisung für die Standesbeamten und ihre Aufsichtsbehörden — DA — vom 16. 4. 1968) folgende Regelung:

„(1) Interessenten kann auf Antrag eine Aufstellung über die beurkundeten Eheschließungen, Geburts- und Sterbefälle gegen angemessenes Entgelt zur Verfügung gestellt werden. In die Aufstellung dürfen nur die Personenstandsfälle aufgenommen werden, mit deren Veröffentlichung sich die Beteiligten einverstanden erklärt haben. Die Angaben sind auf Tag und Ort des Ereignisses (Heirat, Geburt, Tod) sowie auf Vornamen, Familienname, Wohnort und Wohnung der Beteiligten zu beschränken.“

Die Handhabung der z. Z. geltenden Regelung kann unter dem Gesichtspunkt der Wahrung der Persönlichkeitsrechte nicht als befriedigend angesehen werden. Der Datenschutzbeauftragte hat daher in seinen Tätigkeitsberichten wiederholt seine Bedenken dagegen vorgetragen, daß die Verwaltung Informationen, die aufgrund gesetzlicher Bestimmungen der Bürger der Verwaltung zur Verfügung stellen muß, an Dritte weitergibt, vor allem, wenn der Betroffene davon keine Kenntnis hat. Denn nicht immer wird der Betroffene der Dienstausweisung entsprechend um sein Einverständnis gebeten. In anderen Fällen erfolgt die Befragung so beiläufig, oder der Befragte befindet sich dabei in einem Gemütszustand, in dem er die Folgen seiner Einverständniserklärung gar nicht voraussehen kann.

Diese Problematik ist inzwischen auch erkannt worden. Der Bundesminister des Innern hat daher bei den Länderinnenministern die Frage einer Einschränkung dieser Regelung aufgeworfen. Unabhängig davon hat in Hessen das Ministerium für Wirtschaft und Technik das Innenressort darauf aufmerksam gemacht, daß der Verkauf der Anschriften jungvermählter Eheleute oder der Eltern neugeborener Kinder in vielen Fällen zu unseriösen Verkaufspraktiken führe. Es regte an, die Weitergabe von Adressen durch Behörden zu gewerblichen Zwecken zu unterbinden. Das Innenministerium hat in seiner Antwort darauf hingewiesen, daß „für ein Verbot der Auskunftserteilung oder Veröffentlichung ... es z. Z. an einer rechtlichen Grundlage“ fehle. Im Frühjahr 1975 werde aber auf Bundesebene die Frage einer Änderung oder Streichung des § 104 DA erörtert.

Es ist zu begrüßen, daß aufgrund der festgestellten Auswüchse die Weitergabe von personenbezogenen Daten durch öffentliche Stellen gegen Entgelt eingeschränkt werden soll.

## 5. SICHERUNG DES INFORMATIONSGLEICHGEWICHTS

### 5 Sicherung des Informationsgleichgewichts

Die mit dem Vordringen der EDV in der öffentlichen Verwaltung aktualisierte Problematik des Informationsgleichgewichts zwischen Regierung und Parlament — aber auch zwischen Staat und Kommunen — hat in der wissenschaftlichen Diskussion an Gewicht gewonnen. Übereinstimmend wird die Ansicht vertreten, daß ein computerunterstütztes Informationsmonopol der Regierung ihren bereits bestehenden Informationsvorsprung unerträglich vergrößern würde. Deshalb müssen die Informationsrechte des Parlaments gestärkt werden. Das Parlament ist auf die Informationen angewiesen, wenn parlamentarische Gesetzinitiativen entwickelt, Alternativen zu Regierungsentwürfen begründet, das Regierungs- und Verwaltungshandeln parlamentarisch kontrolliert und die Ausführung des Haushaltsplanes zeitnah überwacht werden soll.

#### 5.1 Zugriffsrechte des Parlaments

§ 6 Abs. 1 DSG erweitert das parlamentarische Instrumentarium, mit welchem der Landtag Auskünfte von der Regierung verlangen kann (Große und Kleine Anfrage, Fragestunde, Zitierrecht). Der Landtag kann danach Auskünfte von nachgeordneten Behörden der unmittelbaren und der mittelbaren Landesverwaltung (Landesbehörden, HZD, KGRZ) unmittelbar, d. h. ohne Einschaltung der Landesregierung, verlangen. Dieses Recht steht nicht nur dem Landtagsplenum, sondern auch den in § 6 Abs. 1 genannten Organen des Landtages zu. Dieses Auskunftsrecht gilt jedoch nur für Auskünfte „aufgrund gespeicherter Daten“ und „soweit Programme zur Auswertung vorhanden sind“. Die weitere Beschränkung auf aggregierte oder anonymisierte Daten trägt dem vorrangigen Grundrechtsschutz des Bürgers Rechnung, dessen Persönlichkeitsrecht wegen des Öffentlichkeitsprinzips parlamentarischer Verhandlungen besonders gefährdet wäre, und hat zu Zweifeln keinen Anlaß gegeben. Weiterhin besteht zwischen dem Landtag und der Regierung Einverständnis darüber, daß das Parlament über Auskünfte aufgrund gespeicherter Daten hinaus einen unmittelbaren Zugriff auf Datenbestände der in § 6 Abs. 1 genannten Körperschaften und Behörden in einem noch zu regelnden Verfahren haben muß, weil sonst der kosten- und zeitaufwendige Aufbau parlamentarischer gleichartiger Datenbestände, wie sie der Regierung zur Verfügung stehen, erforderlich wäre.

##### 5.1.1 Ergänzungen des § 6 DSG

Die von der Regierung wiederholt bekundete grundsätzliche Bereitschaft, dem Landtag Zugriff auf verfügbare Datenbestände zu ermöglichen, geht über den Wortlaut des § 6 Datenschutzgesetz hinaus. Eine Anpassung des Gesetzes müßte den unmittelbaren Zu-

gang des Parlaments zu den Datenbeständen von Regierung und Verwaltung verfahrensrechtlich absichern.

Im Zusammenhang hiermit wäre auch zu prüfen, ob die in § 6 Abs. 1 DSG formulierte Voraussetzung „soweit Programme zur Auswertung vorhanden sind“ dem unbestrittenen Bedürfnis des Landtags nach unmittelbarem Zugriff auf Datenbestände der Regierung genügt, und ob damit den technischen Entwicklungen seit dem Inkrafttreten des Datenschutzgesetzes noch hinreichend Rechnung getragen ist. Der Zugang des Landtags zu den Datenbeständen der Regierung — soweit sie nicht zum geschützten Kernbereich gehören — darf jedenfalls nicht davon abhängen, ob die Regierung Auswertprogramme bereitstellt. Der Landtag muß imstande sein, sich die Informationen zu beschaffen, die er benötigt, um Alternativen zu Regierungsvorlagen zu entwickeln und zu begründen; er muß durch Simulationen die Stichhaltigkeit eigener Gesetzesinitiativen überprüfen oder z. B. den „Ist“-Bestand von Einnahmen und Ausgaben aufgrund des Haushaltsplanes in gleicher Weise wie die Regierung abrufen können. Der Zugang des Parlaments zu den Datenbeständen der Regierung würde auch die Kontrolle darüber ermöglichen, ob die Datenbestände eine hinreichende Entscheidungsgrundlage bieten, ob sie fehlerhaft oder ergänzungsbedürftig sind, und ob die Programme zur Auswertung der Datenbestände genügen. Die hierfür erforderlichen Mittel müßte der Landtag sich oder der Regierung bewilligen.

#### 5.1.2 Verhältnis Parlament und HEPAS

Im Berichtszeitraum sind vom Hessischen Datenverbund eine Soziale Infrastrukturdatei, eine Gemeindeplanungsdatei und eine Investitionsdatei aufgebaut worden. Letztere soll alle von der Landesregierung durchgeführten oder geförderten Investitionen erfassen. Neben einer vierteljährlichen Standardauswertung soll sie weitere gezielte Auswertungen möglich machen.

Diese drei Dateien sind wichtige erste Teilstücke des geplanten Hessischen Planungsinformations- und Analysesystems (HEPAS). Sie sind nicht nur für die Landesregierung von Interesse, sondern für alle Institutionen, die nach dem Hessischen Datenschutzgesetz Zugriff zu den in HEPAS gespeicherten Daten erhalten sollen. Das trifft insbesondere für den Landtag zu.

#### 5.1.3 Informationen aus Statistiken

Im Dritten Tätigkeitsbericht wurde dargestellt, daß es zur Sicherung der Informationsfreiheit und des Informationsgleichgewichts erforderlich sei, das Verfahren des Statistischen Landesamtes und die Entwicklung neuer Informationssysteme auf der Grundlage von

Dateien des Verwaltungsvollzugs für den Landesbereich rechtlich zu normieren. Damit sollte vor allem sichergestellt werden, daß auch Parlament und Öffentlichkeit in ähnlicher Weise wie die Regierung alle verfügbaren statistischen Informationen nutzen können. Die Landesregierung hat in ihrer Stellungnahme diesen Punkt nicht für regelungsbedürftig gehalten.

Unabhängig von der Beantwortung der Frage, ob und ggf. wann diese Rechtsetzung erfolgt, hat der Datenschutzbeauftragte aufgrund § 10 Abs. 2 DSGVO die Möglichkeit und die Pflicht, seinen Beitrag zur Sicherung des Informationsgleichgewichts zu leisten. Er wird von sich aus laufend den Entwicklungsstand der amtlichen Statistik und der Informationssysteme überprüfen und darauf hinwirken, daß die vorhandenen Informationen allen Interessierten zur Verfügung stehen. In diesem Zusammenhang verdient die in Berlin mit der Errichtung der Struktur- und Planungsdatenbank (Senatsbeschuß vom 26. 2. 1974) vorgesehene statistische Auskunfts- und Beratungsstelle besondere Beachtung. In dem „Konzept für den Aufbau einer Struktur- und Planungsdatenbank im Rahmen eines Verwaltungsinformationssystems für Berlin (West)“, vorgelegt vom Senator für Inneres, heißt es dazu: „Diese statistische Auskunfts- und Beratungsstelle soll nicht nur einen Überblick über das Programm der Statistik haben, sondern darüber hinaus auch versuchen, andere Informationsquellen, z. B. Geschäftsstatistiken der einzelnen Senatsverwaltungen und in automatisierten Verwaltungsregistern vorhandene Daten für Planungszwecke zu erschließen.“

Auch für Hessen sollte eine vergleichbare Auskunfts- und Beratungsstelle in Betracht gezogen werden. Das erscheint vor allem deshalb von Bedeutung, weil inzwischen weitere planungsrelevante und allgemein interessierende Daten als Ergebnis der Auswertung bestehender Verwaltungsdateien verfügbar sind. Es handelt sich z. B. um Erkenntnisse aus der Besoldungsdatei, die u. a. für den Bereich der Beamten, Altersstruktur, Nachwuchsbedarf und Karriere-Chancen aufzeigen. Allerdings hat man auf anderen Gebieten festgestellt, daß allein das Vorhandensein von Zahlenangaben keine bessere Information bewirkt. Eine grundsätzliche Beratung im Aufspüren und im Umgang mit Informationsquellen ist insbesondere dann erforderlich, wenn der Computer nicht nur als Nachfragestelle benutzt werden soll, sondern gleichzeitig als Hilfe für die Kombination von Daten und für Modellrechnungen. Derartige Modellrechnungen mit mehreren Alternativen sind z. B. interessant bei der Errechnung von Lehrerbedarfszahlen, bei der Fixierung der Modalitäten des kommunalen Finanzausgleichs usw.

#### 5.1.4 Datenbestände des Landes

Ein organisatorisches Datenschutzproblem innerhalb des Datenverbundes rührt an grundsätzliche verfassungs- und verwaltungsrechtliche Fragen: Nach § 5 DSGVO hat jedes Mitglied und jeder Auftraggeber das Zugriffsrecht auf seine Datenbestände (Abs. 1). Durch geeignete Vorkehrungen ist sicherzustellen, daß Daten nicht durch Unbefugte abgerufen werden können (Abs. 3). Die mit dieser Vorschrift begründe-

ten Rechte und Pflichten des Rechenzentrums und seiner Mitglieder und Auftraggeber dienen zugleich dem Datenschutz, weil die Mitglieder und Auftraggeber nur jeweils auf die einzelnen Datenbestände zugreifen können, die sie selbst dem Rechenzentrum gegeben haben. Dritte haben keinen Zugriff. Damit ist einer unkontrollierten Weitergabe insbesondere personenbezogener Daten ein Riegel vorgeschoben.

Soweit es sich um die Gemeinden, die Landkreise, Gemeindeverbände oder andere Auftraggeber (§ 4 Abs. 1 DVG) oder um die KGRZ als Mitglieder handelt, sind Zweifel an der Zugriffsberechtigung kaum denkbar. Anders ist es jedoch bei dem Lande Hessen als Mitglied der HZD (§ 3 DVG). Nach dem Wortlaut des Gesetzes hat derjenige, der das Land Hessen vertritt — das wäre der Ministerpräsident oder der zuständige Minister oder die nachgeordnete Stelle, auf den oder auf die die Vertretungsbefugnis übertragen ist (Art. 103 HV) — Zugriff auf die Datenbestände des „Landes Hessen“. Die Vorschrift könnte dahin ausgelegt werden, daß der Vertretungsberechtigte auf alle Datenbestände des Landes, die es als Mitglied der HZD eingebracht hat, Zugriff habe. Diese Auslegung läge jedoch nicht im Sinne des § 5 DVG, wenn man dessen Absatz 3 und die Vorschriften des Datenschutzgesetzes berücksichtigt.

Eine einschränkende Auslegung erscheint angebracht: Die Delegation der Vertretungsbefugnis nach Artikel 103 HV ist stets ressort- oder aufgabenbezogen. Daher liegt es nahe, auch das Zugriffsrecht auf diejenigen Datenbestände des Landes zu begrenzen, die von den Behörden zur Erfüllung der Aufgaben im Rahmen ihrer Vertretungsbefugnis benötigt werden. Es gibt allerdings keine objektiven Kriterien dafür, welche Datenbestände die Behörden oder Stellen benötigen. Das hängt weitgehend davon ab, in welcher Weise die Vertretungsberechtigten — die Ressorts oder die nachgeordneten Stellen — ihre Aufgaben zu erfüllen beabsichtigen. Eine rechtliche Regelung dieser Frage ist erforderlich. Der HZD, die den Zugriff gewährt, kann die Entscheidung über die Berechtigung zum Zugriff jedenfalls nicht überlassen werden.

Für die Zugriffsbefugnis des Ministerpräsidenten wäre die Sachlage entsprechend. Er hätte ein Zugriffsrecht nur, soweit er die Vertretungsbefugnis nicht delegiert hat. Theoretisch ist zwar die Delegation jederzeit rücknehmbar. Die Vertretungsbefugnis ist jedoch an die Zuständigkeit der Minister oder der nachgeordneten Stelle gebunden (Artikel 103 HV); die Verteilung der Zuständigkeiten innerhalb der Landesregierung unterliegt der — stillschweigenden — Billigung des Landtags und ist daher vor willkürlicher Veränderung gesichert (Art. 104, Abs. 2 HV).

Aus dieser formalen und verfahrensrechtlichen Regelung des § 5 DVG und der Artikel 103 und 104 HV sind materielle Kriterien für die Zugriffsberechtigung auf Datenbestände des Landes Hessen nicht oder nicht mit hinreichender Sicherheit zu gewinnen. Daher ist eine Regelung durch Rechtsverordnung (§ 24 DVG) geboten, in welcher klargestellt wird, ob und unter welchen Voraussetzungen ein Ressort oder eine Behörde der Landesregierung auf Datenbestände ei-

nes anderen Ressorts oder einer anderen Behörde zu greifen kann. Diese Regelung sollte an die Aufgaben, die vom Ressort oder der nachgeordneten Stelle zu erfüllen sind, anknüpfen und, soweit es sich um personenbezogene Daten handelt, Sicherung gegen eine zweckentfremdete Verwendung der vom Bürger erhobenen Daten enthalten.

#### 5.1.5 Auch Bundestag prüft Zugriffsrechte

Auch im Bundestag ist die Frage des Zutritts von Parlamentsmitgliedern zu Datenbanken der Ministerien aktuell geworden. Nachdem der Ausschuß für Forschung und Technologie es abgelehnt hatte, den Forschungsminister aufzufordern, den Ausschußmitgliedern Zutritt zur Datenbank seines Ministeriums zu gewähren, hat die Opposition die Forderung erhoben, daß das Parlament grundsätzlich Einblick in die gespeicherten Daten der Regierung erhalten müsse. In einem von ihr vorgelegten Gutachten wird ein umfassender parlamentarischer Informationsanspruch gegenüber der Regierung und damit der Zugang des Parlaments zu ihren Datenbanken aus dem Grundgesetz abgeleitet. Das Parlament würde in seinen Kontrollfunktionen beeinträchtigt, wenn der herkömmliche Informationsanspruch des Parlaments nicht auf den Direktzugang zu den Datenbanken der Regierung ausgeweitet werde. Eine parlamentarische Arbeitsgruppe aller Fraktionen soll nunmehr die Rechtsgrundlagen für dieses Informationsrecht des Parlaments schaffen<sup>3)</sup>.

#### 5.1.6 Weitergabe von Adressen an Parteien

Als Illustration dafür, daß der Schutz gegen Zweckentfremdung personenbezogener Daten und die Sicherung des Informationsgleichgewichts oft nicht zu trennen sind, ist folgender Vorgang interessant: Das Presse- und Informationsamt der Bundesregierung sammelt in einer Datei die Adressen von Besuchern und von Bürgern, die um Zusendung von Informationsmaterial gebeten haben. Durch Zufall wurde bekannt, daß einer politischen Gruppierung diese Adresse auf Anforderung überlassen wurde. Damit war es ihr möglich, diese Zielgruppe politisch interessierter Bürger mit eigenen Informations- und Werbematerial zu versorgen. Als der Vorfall im Bundestag zur Sprache kam, erklärte der Leiter des Amtes, er habe keine Bedenken gegen die Überlassung dieser Adressendaten an eine Partei. Selbstverständlich ständen die gleichen Adressen auch allen anderen Parteien zur Verfügung. Im Verlauf der Debatte sagte er zu, in Zukunft die

erfaßten Personen davon zu unterrichten, daß ihre Adressen auch politischen Gruppierungen zur Verfügung gestellt werden können. Damit wurden zwei Fragen aufgeworfen:

War das Presse- und Informationsamt befugt, die Anschriften ohne Zustimmung des Betroffenen weiterzugeben?

Wenn derartige Anschriften verfügbar sind, müßte dann diese Tatsache nicht gleichzeitig allen politischen Gruppierungen zur Kenntnis gebracht werden, damit sie ebenfalls in der Lage gewesen wären, diese Anschriften zur Versendung ihres eigenen Materials zu gebrauchen?

#### 5.2 HEPAS-Land und HEPAS-Kommunal

Ein besonderes Problem wirft die im Hessischen Planungsinformations- und Analyse-System (HEPAS) für das Land und für die Kommunen vorgesehene Gleichartigkeit der Datenbasis und Methodensbasis auf. Diese Gleichartigkeit ist notwendig für die Zusammenarbeit von Land und Kommunen. Sie ist zweifellos auch sinnvoll, soweit ein gleichgelagertes Informationsbedürfnis besteht und eine gleiche Interessenlage gegeben ist. Andererseits dürfen durch die Einheitlichkeit des Informations- und Analyse-Systems die spezifischen Planungsbedürfnisse der Kommunalverwaltungen nicht beeinträchtigt werden. Außerdem muß sichergestellt sein, daß die Gemeinden und Gemeindeverbände nicht in einen Informationsrückstand gelangen.

Es muß verhindert werden, daß den Kommunalen Gebietskörperschaften eine für ihre speziellen Interessen weniger aussagefähige Datenbasis als Grundlage für die Informationsgewinnung zur Verfügung steht als dem Land. Konkrete Ansätze hierfür ergeben sich aus einem Vergleich der Konzeption „Hessisches Planungsinformations- und Analyse-System“ für das Land mit den entsprechenden Arbeitsunterlagen für den kommunalen Bereich. „Im Rahmen der für die Kommunalverwaltung geltenden Konzeption für den Aufbau des Hessischen Planungsinformations- und Analyse-Systems im kommunalen Bereich sind die Kraftfahrzeug-Datei und die Einkommens-Datei nicht Bestandteil der Datenbasis, während dies bei der für das Land geltenden Version der Fall ist.“

Die hier zitierte Stellungnahme eines kommunalen Spitzenverbandes verdeutlicht, daß trotz bester Absichten aller am Verbund Beteiligten, insbesondere auch des Landes, die Gefahr von Verschiebungen im Kräfteverhältnis zwischen Land und Kommunen unter Aspekten der EDV durchaus nicht auszuschließen ist.

<sup>3)</sup> Burkhard Dobiey, Zugang des Parlaments zu Datenbanken der Regierung in „Zeitschrift für Parlamentsfragen“ Nr. 3, Oktober 1974, S. 316 ff.



## 6. SCHLUSSBEMERKUNGEN

### 6. Schlußbemerkungen

Bei der Verwirklichung der Datenschutzforderungen handelt es sich nicht nur um den Versuch, den einzelnen Bürger vor Schäden oder zumindest Belästigungen durch Verletzung seiner Privatsphäre zu bewahren. Es geht vor allem auch um die Sicherung und Weiterentwicklung der Grundfreiheiten und der demokratischen Struktur unserer Gesellschaft.

Die Problemstellungen drängen nicht nur zu nationalen, sondern zu umfassenden internationalen Lösungen. Die neuesten Entwicklungen in der OECD, bei den Europäischen Gemeinschaften und beim Europarat geben Grund zur Hoffnung, daß die demokratisch regierten Staaten in der Grundlinie übereinstimmende Lösungen finden werden, wenn es nicht sogar zum Abschluß internationaler Konventionen kommt.

Die internationale Anerkennung grundsätzlicher Datenschutzregeln und die Einsetzung unabhängiger nationaler Institutionen als Überwachungsorgane würde die Chance vergrößern, die jeweiligen Datenschutzvorschriften an die rasante technische Entwicklung und den unaufhörlichen sozialen Wandel anzupassen, damit ungebetene Gäste einer neuen Technologie in Schach gehalten werden können, bevor unaufhebbarer Schäden entstehen.

Obwohl dies Ziel sehr hoch gesteckt erscheinen mag und seine Erreichung ungewiß ist, sollte jede Möglichkeit, sich ihm zu nähern, genutzt werden. Wie notwendig es ist, die Gefahren zu erkennen, die sich hinter einer faszinierenden Ausnutzung der Computertechnik verbergen, dafür ist die NEW YORK TIMES-INFORMATIONSBANK ein besonders aufschlußreiches Beispiel.

Einzelheiten über diese Informationsbank wurden in dem Interview eines Beauftragten der DIEBOLD EUROPA SA mit dem Leiter der NEW YORK TIMES-Informationsbank geschildert, das auf die Anregung eines Mitarbeiters des Presse- und Informationsamtes der Bundesregierung Bezug nimmt und in der Ausgabe von Januar/Februar 1975 der Zeitschrift DATA EXCHANGE veröffentlicht worden ist. Derartige Informationsbanken verstärken die Zentralisierungstendenzen erheblich und vergrößern die Machtkonzentration im publizistischen Bereich in gefährlicher Weise. Es ist außerordentlich bedenklich, daß diese Entwicklung bisher auf wenig kritische Aufmerksamkeit gestoßen ist. Dies scheint Blindheit gegenüber den Auswirkungen einer bedenkenlosen Ausnutzung der Technik auf die demokratische Struktur unserer Gesellschaft zu offenbaren.

Begonnen hat die Entwicklung mit dem berühmten „NEW YORK TIMES-INDEX“, einem nach vielen tausend Suchbegriffen computergerecht aufbereiteten Inhaltsverzeichnis für alle Ausgaben der NEW YORK TIMES seit der Gründung vor mehr als 100 Jahren. Zusammen mit der Mikroverfilmung der NEW YORK TIMES erlaubt es das System, jede Meldung bzw. jeden Bericht im Originaltext zur Kenntnis zu nehmen oder abzulichten. Das System kann nicht nur von den eigenen Redaktionen bzw. allen Redaktionen des NEW YORK TIMES-Konzerns in Anspruch genommen werden. Es steht auch gegen Gebühren jedermann über direkte Abfrage-Terminals zur Verfügung. In wenigen Sekunden kann man

jeweils über Detail- und Hintergrundinformationen verfügen, die man sich sonst in mehr oder weniger gut bestückten Archiven mühsam zusammensuchen müßte.

Inzwischen hat diese Informationsbank auch aus dem Inhalt weiterer maßgeblicher Publikationsorgane Informationen aufgenommen. Dabei handelt es sich um Zeitungen wie WASHINGTON POST, LOS ANGELES TIMES, THE WALLSTREET JOURNAL und die Londoner TIMES, außerdem um Wochenmagazine, Wochenzeitschriften, Spezialzeitschriften für Wirtschaft, Kunst und Außenpolitik. Die Veröffentlichungen aus diesen Informationsträgern sind in der NEW YORK TIMES-Informationsbank nicht nur in der Form eines Index, sondern auch in der Form von sogenannten „abstracts“, d. h. ausgeschriebenem Zusammenfassungen der jeweiligen Sachaussage mit Hinweisen auf die Originalveröffentlichung gespeichert.

Die Entwicklung wird mit großer Wahrscheinlichkeit dahin führen, daß sich Zeitungen und Zeitschriften, Funk- und Fernsehgesellschaften, wissenschaftliche Bibliotheken und Dokumentationszentren oder die Hauptverwaltungen von Wirtschaftsunternehmen, große Verbände und die oberen Etagen der Behörden in Zukunft jeweils dieselben grundlegenden Informationen verschaffen. Was das für die Vorstrukturierung der öffentlichen Meinung bedeutet, ist kaum absehbar.

Die für den Erfolg einer solchen Einrichtung erforderlichen Vorleistungen im Hinblick auf Zeit und Geld sind so umfangreich, daß man z. B. in der Bundesrepublik für die Errichtung einer ersten und möglicherweise auf längere Sicht einzigen Informationsbank auf Computerbasis die potentiellen Kapitaleigner an einer Hand wird abzählen können.

Die NEW YORK TIMES hat mit ihren Vorarbeiten bereits in den Jahren 1965/66 begonnen. Außenstehende Kunden wurden ab Februar 1973 angenommen. Einer der ersten Kunden war die CIA (Central Intelligence Agency). Inzwischen werden eine Reihe von amerikanischen Zeitschriften, internationalen Nachrichtenagenturen, Radio- und Fernsehanstalten sowie Wirtschaftsunternehmen, Wirtschaftsverbänden und Regierungsstellen, außerdem natürlich Hochschulen, etc. beliefert. Nach dem Interview gehört zu den Abonnenten aus Deutschland auch die Illustrierte STERN.

Wenn man in Betracht zieht, daß der Leiter der Informationsbank, Rothman, im Interview vorbehaltlos die Meinung äußerte, daß die in der Bank gespeicherten Daten über Einzelpersonen keine Gefährdung des Persönlichkeitsrechts darstellen könnten, weil es sich doch ausschließlich um veröffentlichte Daten handle, so stellt sich die Frage, ob sich das allein mit Naivität erklären läßt. Man braucht sich nur auszumalen, welche Auswirkungen es auf die Meinungsfreiheit haben und welcher Einschüchterungseffekt sich ergeben würde, wenn in Sekundenschnelle ein Bericht erstellt werden könnte, der Meinungsäußerungen eines einzelnen in verschiedenen Situationen, sein persönliches Verhalten bei verschiedenen Anlässen oder sonstige individuelle Verhaltensweisen zusammenfaßt.

Diese Gefahr besteht nicht allein für die Meinungsfreiheit, sondern für die Freiheitsrechte schlechthin. Sie fordert Gegenmaßnahmen heraus.



## DATENVERKEHRS-ORDNUNG

10 Gebote einer Datenverkehrs-Ordnung  
(vgl. Stenographischen Bericht des Hess. Landtags 7/97 vom  
28. August 1974, S. 5227 f.)

Auf der Grundlage eines Fairness-Kodex, der eine Art Konsensus dessen darstellt, was in einer modernen demokratischen Gesellschaft unter fairem Umgang mit Informationen zu verstehen ist, und der für alle Arten der Informationsverarbeitung gilt, sind die Auskunfts- und Abwehrrechte des Bürgers in der elektronischen Datenverarbeitung (EDV) in einer Datenverkehrs-Ordnung niederzulegen, die etwa folgende 10 Gebote enthalten muß:

1. Der Einsatz der elektronischen Datenverarbeitung darf die individuellen und kollektiven Freiheitsrechte des Bürgers nicht gefährden.
2. EDV-Systeme für personenbezogene Daten müssen öffentlich bekannt sein; es darf keine geheimen Systeme geben.
3. Wer personenbezogene Daten in EDV-Anlagen verarbeitet, muß durch ausreichende Sicherungsmaßnahmen den Mißbrauch der Daten verhindern.
4. Jeder Bürger muß das Recht und die Möglichkeit haben, Auskunft darüber zu erhalten, an welcher Stelle welche Informationen über ihn gespeichert sind, wofür sie verwendet und an wen sie weitergegeben werden.
5. Jeder Bürger muß das Recht haben, die über ihn gespeicherten Daten zu berichtigen und zu ergänzen.
6. Wer vom Bürger Daten verlangt, muß ihm die Rechtsgrundlage dafür nennen oder auf die Freiwilligkeit der Auskunft hinweisen. Widerrechtlich gespeicherte personenbezogene Daten müssen auf Verlangen des Betroffenen gelöscht werden.
7. Personenbezogene Informationen, die zweckgebunden gegeben worden sind, dürfen ohne Zustimmung des Betroffenen nicht für andere Zwecke verwendet oder weitergegeben werden.
8. Für die Benutzung von Dateien, deren Daten dem Betroffenen nicht bekanntgegeben werden können — z. B. in den Informationssystemen der Polizei und Nachrichtendienste — müssen Rechtsnormen festgelegt werden.
9. Für die Speicherung von personenbezogenen Daten müssen Lösungsfristen bestimmt werden, wobei die Schutzrechte des Bürgers und die Informationsrechte der Allgemeinheit zu einem Ausgleich gebracht werden.
10. Die Nutzung der EDV darf bestehende oder entstehende Machtvorsprünge nicht derart erweitern oder verfestigen, daß dadurch ein demokratischer Machtausgleich erschwert oder gar verhindert wird.



## SACHVERSTÄNDIGENANHÖRUNG DES BUNDESTAGS-INNENAUSSCHUSSES

Schriftliche Stellungnahme des Hessischen Datenschutzbeauftragten bei der Sachverständigenanhörung des Innenausschusses des Bundestages am 6. Mai 1974.

### D. Überwachung des Datenschutzes

Frage: 1. Halten Sie die Einrichtung einer Institution, die die Einhaltung der Vorschriften des BDSG in allen Anwendungsbereichen überwacht, für erforderlich?

1. Die Einrichtung von Institutionen, welche die Einhaltung der Vorschriften des BDSG überwachen, ist erforderlich. Eine einzige Institution ist dafür faktisch und rechtlich ungeeignet.

Die Voraussetzungen für eine Kontrolle sind in den einzelnen Anwendungsbereichen verschieden. Es sind zu unterscheiden:

- Die Zulässigkeitsvoraussetzungen für die Datenverarbeitung von den Abwehrrechten des Bürgers und den Anmeldepflichten der Datenverarbeiter;
- Der Bereich der öffentlichen Verwaltung des Bundes von dem Bereich der Länder und von dem nicht-öffentlichen Bereich.

- 1.1 Nach dem Regierungsentwurf soll die Verarbeitung personenbezogener Daten (Speichern, Verändern, Weitergeben) unter einem allgemeinen Verbot mit Erlaubnisvorbehalt stehen.

Sie soll nur, wenn das DSG oder ein anderes Gesetz sie erlaubt oder wenn der Betroffene zugestimmt hat, zulässig sein (§ 2 Abs. 3).

- 1.1.1 Eine institutionalisierte Kontrolle darüber, ob die Zulässigkeitsvoraussetzungen im Einzelfall gegeben sind, ist nicht vorgesehen.

Die Beurteilung, ob die Datenverarbeitung im Rahmen der rechtmäßigen Erfüllung zuständiger Aufgaben (öffentlicher Bereich) liegt oder im Rahmen eines Vertragsverhältnisses etc. erfolgt, mußte von der datenverarbeitenden Stelle entschieden werden.

- 1.1.2 Insoweit ist die Konzeption des Regierungsentwurfs sowohl unter dem Blickpunkt des Grundrechtsschutzes des Bürgers zu kritisieren, als auch vom Standpunkt des technischen Fortschritts und seiner Ausnutzung für die Verwaltung aller Bereiche bedenklich.

Einerseits ist es wegen der notgedrungenen in Generalklauseln ausweichenden Regelung von Zulässigkeitsvoraussetzungen praktisch unmöglich, wirksam darüber zu wachen, ob jede Datenverarbeitung personenbezogener Daten im öffentlichen oder im nicht-öffent-

lichen Bereich nach den gesetzlichen Voraussetzungen zulässig ist.

Andererseits ist es erfahrungsgemäß aussichtslos und daher verfehlt, die Ausnutzung des technischen Fortschritts in der Elektronik mit ihren großen Vorteilen sowohl für die Verwaltungen aller Bereiche als auch für das Gemeinwohl und den einzelnen in der Weise zu reglementieren und zu beschränken, daß die Zulässigkeit der Datenverarbeitung von einer besonderen Erlaubnis abhängig gemacht wird.

- 1.1.3 Die Alternative zu dieser Konzeption ist die prophylaktische Begleitung und Absicherung der fortschreitenden Automation der Verwaltung mit flankierenden Vorschriften und Maßnahmen des Datenschutzes mit der Maßgabe, daß die Sicherung des Grundrechtsschutzes grundsätzlich den Vorrang vor den mit der Automation zu erzielenden Erleichterungen der Verwaltung hat. Maßstab für die Zumutbarkeit der Datenschutzforderungen muß der Grad der Gefährdung des Grundrechtsschutzes durch die Automation, darf dagegen nicht — wie in § 4 I BDSGE — der Aufwand sein, den der Datenschutz erfordert. Mit anderen Worten: statt des Verbots mit Erlaubnisvorbehalt die Zulassung mit Genehmigungsvorbehalt. Unter diesem Gesichtspunkt gewinnen auch die — richtigerweise vorgesehenen — Meldepflichten (§ 30 BDSGE) volles Gewicht, weil die Aufsichtsbehörde befugt wäre, die Genehmigung der angemeldeten EDV-Tätigkeiten von Auflagen abhängig zu machen, die der jeweiligen Sachlage entsprechen.

- 1.2 Die Erfordernisse einer Überwachungsinstitution sind — unter dem Blickpunkt des Grundrechtsschutzes — im öffentlichen Bereich anders als im nicht-öffentlichen Bereich.

- 1.2.1 Der öffentliche Bereich steht unter den Verfassungsgrundsätzen des Rechtsstaats, insbesondere der Gewaltenteilung, der parlamentarischen Verantwortlichkeit und der Gesetzmäßigkeit der Verwaltung. Die überkommenen Verwaltungsmittel, die — abgesehen von der Rechtsweggarantie und der Dienstaufsicht — dem Schutze des Bürgers zu dienen bestimmt sind, insbesondere Amtsgeheimnis und Verschwiegenheitspflicht der Bediensteten, müssen den spezifischen Gefahren der EDV angepaßt werden.

Die Eigen-Kontrolle der behördlichen Tätigkeit bietet dem Bürger bei Interessenkonflikten keine Sicherheit dafür, daß seine Interessen die gebührende Berücksichtigung gegenüber dem Interesse der Verwaltung finden. Die nachträgliche Kontrolle durch die Gerichte oder durch die Dienstaufsicht hilft nicht, einen

Schaden von vornherein zu verhindern. Richtiger ist, eine vorbeugend wirkende Überwachung der EDV in der Verwaltung durch eine außerhalb stehende unabhängige Stelle zu garantieren.

- 1.2.2 Dies gilt sowohl für die Bundesverwaltung als auch für die Verwaltungen der Länder. Jedoch kann nicht eine einzige Institution den gesamten Verwaltungsbereich des Bundes und der Länder abdecken.

Abgesehen von den noch zu erörternden verfassungsrechtlichen Gründen wäre eine einzige Institution auch wegen des Umfangs der Überwachungsaufgaben überfordert. Die Größe des erforderlichen Verwaltungsapparates würde der aktuellen Wirksamkeit und Flexibilität der Kontrollinstanz entgegenwirken.

Außerdem könnte sich eine solche zentrale Datenschutzinstitution wegen ihres Einflusses nicht zuletzt auch auf die Meinungsbildung in der Öffentlichkeit, zu einem Machtzentrum entwickeln und die gewaltenteilende Funktion des Bundesstaatsprinzips empfindlich stören.

Daher sind für den Verwaltungsbereich des Bundes und für den jedes Landes eigenen Überwachungsinstitutionen zu schaffen.

- 1.3 Für die Überwachung des Datenschutzes im nicht-öffentlichen Bereich gelten andere Maßstäbe als im öffentlichen Bereich. Ziel des Datenschutzes ist zwar auch hier, die sich aus Artikel 1 Abs. 1 und Artikel 2 Abs. 1 GG ergebende Grundrechtsposition des Einzelnen gegen Eingriffe abzuschirmen. Jedoch sind Maßstäbe für die Zulässigkeit der Eingriffe nicht — wie im öffentlichen Bereich — die Gesetzmäßigkeit der Verwaltung und die Sozialgebundenheit der Bürger, sondern die Rechte Dritter, die sich u. a. aus der allgemeinen Handlungsfreiheit nach Artikel 2 Abs. 1 GG, aus der Informationsfreiheit nach Artikel 5 Abs. 1 GG und aus der Freiheit der Berufsausübung nach Artikel 12 Abs. 1 GG ergeben. Einerseits erfordern die spezifischen Gefahren, die mit der EDV für den Einzelnen gerade auch im Bereich der Wirtschaft verbunden sind, entsprechende Schutzmaßnahmen; andererseits müssen die Beschränkungen und Begrenzungen der Verwendung von EDV-Anlagen die grundrechtlich geschützten Positionen der Datenverarbeiter berücksichtigen. Diese Abwägung kann wegen der unvermeidbaren Interessenkonflikte nicht den datenverarbeitenden Unternehmen überlassen bleiben.

Der Entwurf sieht nur für einen Teilbereich eine Meldepflicht der Datenverarbeiter (§ 30) und eine Aufsicht durch Landesbehörden (§ 31) vor; die Regelung muß für den gesamten nicht-öffentlichen Bereich gelten.

- 1.3.1 Die Aufsicht durch staatliche Behörden macht die Überwachung des Datenschutzes durch eine unabhängige Datenschutzeinrichtung nicht überflüssig.

Die EDV ist eine in rascher Entwicklung befindliche Technik. Sie entwickelt fortlaufend neue Formen und Möglichkeiten der Datenverarbeitung. Diese Entwicklung und ihre Auswirkungen auf den Grund-

rechtsschutz des Einzelnen — die weiteren Folgewirkungen für die verfassungsmäßige Struktur in Bund, Ländern und Gemeinden werden hier außer Acht gelassen — müssen mitlaufend beobachtet und überprüft werden, damit Entwicklungstendenzen rechtzeitig erkannt und vorbeugende Maßnahmen angeregt werden können. Für eine solche auf das Allgemeine ausgerichtete, den Einzelfall nur als Beispiel verwertende Beurteilung sind die Aufsichtsbehörden schon deshalb ungeeignet, weil ihnen wegen ihres regional begrenzten Zuständigkeitsbereiches der nötige Überblick fehlt.

- Frage: 2. Wie müßte diese Institution nach Ihrer Auffassung etwa organisatorisch gegliedert und personell ausgestattet sein, damit sie ihre umfassenden Kontroll- und Überwachungsaufgaben wirksam durchführen kann? Welche rechtlichen Möglichkeiten zur Schaffung dieser Institutionen bestehen

- a) ohne Grundgesetzänderung?  
b) mit Grundgesetzänderung?

2. Die Datenschutz-Überwachungsinstitutionen wären unter Beachtung folgender Gesichtspunkte zu organisieren:

- Im öffentlichen Bereich sind für den Bund und für jedes Land eigene Institutionen einzurichten.
- Diese Institutionen müssen von der Verwaltung unabhängig sein, einen unmittelbaren Zugang zur Öffentlichkeit und das Recht zur unmittelbaren Berichterstattung an das Parlament haben.
- Im nicht-öffentlichen Bereich muß der Datenschutz von der jeweils zuständigen Landes- oder Bundesbehörde gewährleistet werden. Die Ämter müssen gesetzlich ermächtigt sein, bestimmte Aufgaben zu machen und deren Erfüllung bei den Datenverarbeitern mit den üblichen Verwaltungsmitteln durchzusetzen.
- Die Gesetzgebung auf dem Gebiet des Datenschutzes muß koordiniert werden. Die Datenschutzregeln müssen im Bundesgebiet nach einheitlichen Gesichtspunkten angewandt werden. Diese Koordinations- und Kooperations-Aufgaben sind den Überwachungsinstitutionen für den öffentlichen Bereich zu übertragen.
- Die rechtliche Verantwortung für die Gewährleistung des Datenschutzes muß im öffentlichen Bereich bei den datenverarbeitenden Behörden und Stellen, im nicht-öffentlichen Bereich bei den Aufsichtsbehörden verbleiben.
- Die personelle Ausstattung kann in einem kleinen Rahmen gehalten werden.

Die Einrichtung solcher Datenschutz-Überwachungsinstitutionen ist ohne Änderung des Grundgesetzes zulässig.

- 2.1 Die Organisation des Datenschutzes im Bereich der öffentlichen Verwaltung des Bundes und der Länder gehört zur ausschließlichen Zuständigkeit dieser Gebietskörperschaften. Es widerspräche dem bundes-

- staatlichen Aufbau der Bundesrepublik, einer Bundesinstanz die Überwachung von Behörden und Stellen der Länder hinsichtlich der Gewährleistung des Datenschutzes zu übertragen. Eine Bundesaufsicht ist nur nach Maßgabe des § 84 Abs. 5 und des § 85 Abs. 3 und 4 GG zulässig und erstreckt sich nur auf die Ausführung von Bundesgesetzen durch die Länder als eigene Angelegenheit oder im Auftrage des Bundes. Datenschutz in der öffentlichen Verwaltung umfaßt jedoch auch den weiten Bereich der Regierungs- und Verwaltungstätigkeit, die neben der Ausführung von Bundesgesetzen vollzogen wird.
- 2.2 Die Wirkungsmöglichkeiten jeder Überwachungsinsti-  
tution sind einerseits davon abhängig, wie stark  
oder wie gering ihre Verflechtung mit den Behörden  
und Stellen ist, die sie zu überwachen hat. Deswegen  
haben die Mitglieder der Rechnungshöfe die persön-  
liche Unabhängigkeit wie die Richter. Zum anderen  
hängt die Wirkungsmöglichkeit der Überwachung da-  
von ab, an wen die Institution ihre Feststellungen und  
Anregungen richten kann. Deswegen werden die Prü-  
fungsberichte der Rechnungshöfe auch veröffent-  
licht.
- In gleicher Weise muß die Datenschutz-Überwa-  
chungsinstitution unabhängig sein und den unmittel-  
baren, nicht über die Regierung geleiteten Zugang  
zum Parlament und zur Öffentlichkeit besitzen.
- 2.3 Im nicht-öffentlichen Bereich wird das Prinzip der  
Fremdkontrolle dadurch verwirklicht, daß die Daten-  
schutzaufsicht Landes- oder Bundesbehörden über-  
tragen wird, wie es der Regierungsentwurf auch für  
einen Teilbereich vorsieht.
- Das geeignete Mittel, die Anforderungen des Daten-  
schutzes bei den Datenverarbeitern durchzusetzen, ist  
das behördliche Genehmigungsverfahren, verbunden  
mit der Pflicht, DV-Anlagen der Aufsichtsbehörde zu  
melden, und mit der Befugnis der Behörden, Geneh-  
migungen zum Betrieb von DV-Anlagen von Aufla-  
gen abhängig zu machen, die gesetzlich bestimmt sein  
müssen.
- Unabhängig vom Rechtsweg und von der Dienstauf-  
sicht der vorgesetzten Behörden muß die Daten-  
schutz-Überwachungsinstitution befugt sein, von den  
Aufsichtsbehörden Auskünfte über alle Fragen des  
Datenschutzes im nicht-öffentlichen Bereich zu for-  
dern und sie in den Berichten an das Parlament und  
an die Regierung zu verwerten.
- 2.4 Die Gesetzgebung auf dem Gebiet des Datenschutzes  
sollte im Bereich der Bundesrepublik auf übereinstim-  
menden Grundlagen beruhen.
- Die gesetzlichen Datenschutzregeln sollten darüber  
hinaus bundeseinheitlich angewandt werden. Dies er-  
fordert eine Zusammenarbeit von Bund und Ländern  
in ähnlicher Weise, wie sie auf vielen anderen Gebie-  
ten stattfindet.
- Koordination und Kooperation sind Aufgaben, die  
den Datenschutz-Überwachungsinstitutionen, die im  
Bund und in den Ländern für den öffentlichen Bereich  
einzurichten sind, übertragen werden sollten.
- 2.5 Zusammengefaßt ergibt sich folgende Organisation:  
Die Beachtung des gesetzlich geregelten Datenschut-  
zes im Einzelfall und beim Aufbau von Datenbanken  
und Informationssystemen liegt in der Verantwortung  
der datenverarbeitenden Behörden und Stellen der öf-  
fentlichen Verwaltung und der Aufsichtsbehörden für  
den nicht-öffentlichen Bereich.
- Daneben überwachen unabhängige Datenschutzbe-  
auftragte (-Ausschüsse), die Entwicklung der Auto-  
mation im öffentlichen und im nicht-öffentlichen Be-  
reich, jeweils für das Gebiet ihres Landes bzw. für die  
Bundesverwaltung.
- Das Schwergewicht ihrer Aufgabe liegt in der Unter-  
stützung des Bürgers bei der Wahrnehmung seiner  
Datenschutzrechte, im Aufzeigen von Fehlentwick-  
lungen, in der Erarbeitung von Empfehlungen und  
Vorschlägen an die für den Datenschutz verantwort-  
lichen Behörden und Stellen sowie in Berichten an  
Parlament und Öffentlichkeit.
- Die Datenschutzbeauftragten (-Ausschüsse) koope-  
rieren, d. h. sie tauschen ihre Erfahrungen unterein-  
ander aus, verständigen sich über die Auslegung und  
Anwendung gesetzlicher Datenschutzvorschriften,  
vereinbaren gemeinsame Richtlinien für die Gewähr-  
leistung des Datenschutzes und stimmen sich über  
Vorschläge und Anregungen an die Parlamente und  
Regierungen zur Verbesserung des Datenschutzes in  
gemeinsamen Konferenzen der Datenschutzbeauf-  
tragten (-Ausschüsse) ab.
- 2.6 Bei dieser Konzeption erfordern Datenschutz-Über-  
wachungsinstitutionen nur eine geringe personelle  
Ausstattung, da sie mangels Anweisungsbefugnissen  
und Eingriffs- oder Anordnungsrechten keine Verwal-  
tungsbehörden herkömmlicher Art sind.
- Ihre Tätigkeit besteht im wesentlichen in der Samm-  
lung möglichst umfassender Informationen über die  
Entwicklung der EDV und über die Fortschritte der  
Automation im In- und Ausland, in der Auswertung  
ihrer Erkenntnisse und in deren Vermittlung an Da-  
tenverarbeiter sowie an Hersteller von DV-Anlagen  
und Software-Produzenten.
- Die Größe des Stabes dieser Datenschutz-Überwa-  
chungsinstitutionen wird sich im großen und ganzen  
nach der Einwohnerzahl und der wirtschaftlichen  
Struktur des Landes richten.
- Zur Illustration: Die Dienststelle des Hessischen Da-  
tenschutzbeauftragten ist zur Zeit mit je einer Stelle  
A16, A14, A13 sowie mit zwei Stellen für Schreib-  
kräfte ausgestattet. Daneben stehen dem Daten-  
schutzbeauftragten zur Zeit Mittel für Sachverständi-  
ge in Höhe von DM 40.000 jährlich zur Verfügung.
- 2.7 Die Verwirklichung der vorgeschlagenen Konzeption  
erfordert keine Grundgesetzänderung.
- 2.7.1 Eine Grundgesetzänderung wäre erforderlich, wenn  
eine Bundesinstitution Kompetenzen auch im öffent-  
lichen Bereich der Länder besitzen sollte und wenn ihr  
von Artikel 84 und Artikel 85 GG abweichende Auf-  
sichtsbefugnisse zustehen sollten. Hierbei wäre Arti-  
kel 79 Abs. 3 GG zu beachten.

- 2.7.2 Eine Grundgesetzänderung wäre ferner erforderlich, wenn man die Unabhängigkeit der Bundesinstitutionen verfassungsrechtlich absichern wollte. Dies könnte erwünscht sein, weil die Möglichkeit ausgeschlossen würde, die nur durch ein einfaches Gesetz verbürgte Unabhängigkeit auf dem gleichen Weg abzuschaffen oder einzuschränken.
- 2.7.3 Schließlich wäre eine Grundgesetzänderung mit dem Ziel, der unabhängigen Datenschutzinstitution Weisungs- oder Anordnungsbefugnisse gegenüber den obersten Bundesbehörden oder den ihnen nachgeord-

neten Behörden und Stellen zu verleihen, unzulässig, weil verfassungswidrig.

Da die Unabhängigkeit der Datenschutzinstitution sie aus dem Verwaltungsaufbau der obersten Bundesbehörden ausgegliedert und deren Machtbereiche entzieht, würden Weisungsbefugnisse der Datenschutzinstitution gegenüber der Verwaltung die parlamentarische Verantwortlichkeit der Minister einschränken. Die obersten Bundesbehörden wären keine obersten Behörden mehr; denn sie müßten in Fragen des Datenschutzes der Datenschutzinstitution weichen.

## SACHWÖRTERVERZEICHNIS

(I, II, III und IV bezeichnen den Ersten, Zweiten, Dritten bzw. Vierten Tätigkeitsbericht, die arabischen Ziffern die Abschnitte der Berichte).

Adressenhandel	II 1.3.2 III 1.5.6 IV 1.6, IV 2.2.2, IV 4.7.8, IV 5.1.6	Auskunftspflicht	II 1.3 IV 1.5.1
Alarmpläne	II 4.3.1	Auskunftsrecht des Bürgers	I 2.2.1, I 4.1.4 II 4.1.4 III 1.5 IV 1.5.1, IV 1.6, IV 3.1, IV 4.7.2
Allwissenheit des Staates	I 1.2.1	Auskunftssystem	III 4.1.3
Amtshilfe und Datenschutz	I 4.1.2 II 4.1.1.1 b III 1.5.5, III 5.3 IV 1.5.2, IV 4.6	Automation, Nutzen der —	I 1.2.2, I 1.2.3
Analyse (Ist- und Soll-)	II 4.2.2	Baader-Meinhof-Report	III 1.2.2
Anonymisierung	IV 4.7.2	Baden-Württemberg, Datenschutz in —	I 2.1.5, I 4.2.1
Anregungen	I 5. II 5. III 5. IV 1.1, IV 1.2, IV 1.5.2, IV 3.2, IV 4.3, IV 4.5, IV 4.5.1, IV 4.6, IV 4.7.5, IV 4.7.6, IV 5.1.1, IV 5.1.3, IV 5.1.4, IV Anlage I	Bankgeheimnis und Datenschutz	I 4.1.1.3 d
Arbeitsgruppe EDV des Landtags	III 4.2	Baskir, L.	II 4.1.1.1
Anrufungsrecht des Bürgers (§ 11 DSG)	I 4.1.4, I 5.10 II 4.1.4 III 1.3 IV 1.6	Bayern, Datenschutz in —	I 2.1.2, I 2.4.2
Arbeiter-Samariter-Bund	III 4.1.1.2	Bebauungsplan	IV 4.7.2
Ausbildung im Datenschutz	I 5.8 II 4.2.2 III 5.	Befragungen	IV 1.6, IV 1.7, IV 4.7, IV 4.7.5, IV 4.7.8
Auskunfteien	II 1.3 IV 2.2.3	Benutzerfreundlich	II 1.1
Auskunftsersuchen des Parlaments	I 4.2.3 III 4.2.1 IV 5.1	Bereich des Gesetzes	I 4.1.3 II 4.1.3
Auskunft, Freiwilligkeit der —	III 4.1 IV 4.7.5 IV Anl. I	Bereichsspezifische Regelung	III 1.5.1, III 5.1 III 1.5.3 IV 1.5.2
		Berichtigungsanspruch des Bürgers	I 2.2.1 III 1.5 IV 1.5.1
		Berlin, Datenschutz in —	I 2.1.8 III 2.1.8
		Bestandsaufnahme — der Behörden und Stellen	I 3.1 II 3.1 III 3.
		Beurteilung der — — der maschinellen Datenverarbeitung	I 3.2 II 3.2 I 1.1
		Bestechung	III 1.3, III 3.4.1
		Betroffenenfreundlich	II 1.1

Betroffener		Computerkriminalität	I 4.3.2
Benachrichtigung des —	II 2.4.3,		III 1.3,
Einzelauskunft an —	II 4.1.1.3 g		III 4.3.1
Rechte des —	III 1.5,	Computermißbrauch-Versicherung	II 1.3
	III 4.1.1,		
	III 4.1.2		
Bibliothekswesen	IV 4.7.7	DAMM	III 1.2
Bistümer, kath.	II 4.1.1.3 f	Dammann/Karhausen/Müller/Steinmüller	III 2.2.1
Bremen, Datenschutz in —	I 2.1.8	DASCH	II 4.1.1.3,
Bühnemann	III 2.2.1		II 4.3.1
Bund			III 4.3.1
Datenschutzgesetzgebungsstand im —	I 2.2,		IV 1.5.1,
	I 5.1.1		IV 4.2,
	III 2.2		IV 4.5.2
Bundesangestelltentarif (BAT — § 9)	II 4.1.1.1	Datainspektionen	III 2.3.5
Bundesanstalt für Arbeit	II 4.1.1.1 b,	Daten	IV 2.2.2
	II 4.1.1.2	—artenkatalog	II 1.4
Bundesausbildungsförderungsgesetz	I 4.1.1.2		IV 3.1
Bundesdatenschutzgesetz		Einwohner —	I 2.2.1
—Initiativ-Entwurf	I 2.2.2,	Grund —	I 1.2.1
	I 2.4.7	„harmlose“ —	I 1.2.3
—Regierungsentwurf	I 2.2.3	Individual —	I 1.2.1
	II 1.3,		IV 3.1,
	II 2.4.1,		IV 4.7,
	II 4.1.1		IV 4.7.7
	III 1.2,	personenbezogene — (s. Personen-	
	III 1.4,	bezogene Daten)	III 1.5.1
	III 2.2.1,	sachbezogene —	I 4.1.3.2
	III 2.2.2	—weitergabe an andere Behörden	I 2.2.1,
	IV 1.5.2,		I 5.4
	IV 2.1		III 1.5.5
Bundesgesetze und Datenschutz	I 4.1.1.1,	—weitergabe außerhalb der Verwaltung	IV 3.1
	I 4.1.1.2		III 1.5.6
	III 2.2.1,		IV 4.7.8,
	III 2.2.2		IV 5.1.6
Bundeskriminalamt	III 4.1.5.1	— an Religionsgesellschaften	II 4.1.1.3 f
	IV 4.5.1		III 4.1.6
Bundesmeldegesetz	I 2.2.1	medizinische —	II 4.1.2.1,
	II 2.2.1		II 4.1.2.3
	III 2.2.1,		III 4.1.1
	III 2.2.2	—zweckentfremdung	II 4.1.1.1 c
	IV 2.1	Datenaustausch	II 1.3.2
Bundespost	II 4.1.1.3 g	Datenbanken	I 1.2.1,
Bundesrecht, Kollision mit —	I 1.3.2		I 1.2.3
Bundesregierung	I 1.2.3		II 4.1.1.1 c
	III 2.2.1,		III 1.5.2
	III 2.2.2	Einwohnerwesen —	III 4.1.3
Bundestag	IV 5.1.5	hochschulspezifische —	I 4.1.1.1,
Entschließung des — vom 21. 6. 1972	II 4.1.1.2		I 4.1.1.2
Bundesverfassungsgericht (Mikrozensus)	I 1.2.3	medizinische —	III 4.1.1.3
	III 1.2.2	Personal —	III 4.1.2
— Ehescheidungsakten-Urteil	II 4.1.1.6	—register	I 2.4.3
	III 1.5.5		II 2.4.3
— Lebach-Urteil	III 4.1.5.1		III 1.5.2,
Bußgeldvorschriften	I 2.2.4,		III 5.6
	I 2.4.6		IV 1.5.1,
Bundeszentralregistergesetz	II 4.1.1.3 c	statistische —	IV 3.
	IV 4.5,		I 4.1.1.1
	IV 4.5.1		

Datenerfassung für die Unterlagen	I 4.1.1.1	Aufgaben des —	II 4.1.2.1
Datenfernverarbeitung	I 1.2.3		III 4.1
	III 2.5	Aufgabenbereich des —	I 4.1.3,
	IV 3.2,		I 4.1.3.2
	IV 4.		IV 4.3
Datengeheimnis	II 4.3.1,	— und privatrechtliche Organisationen	II 4.1.3.2
Datenmißbrauch	II 1.3.1,	der öffentlichen Hand	III 1.5.1,
	II 2.2.4		III 5.1
	III 1.2.1	Datenschutzgesetz	
Datenschutz	I 1.1,	hessisches —	I 1.1,
	I 1.4.3		I 1.3,
— außerhalb Hessens	I 2.		I 2.2.4,
	II 2.		I 2.4,
	III 2.		I 2.4.1,
— im Ausland	III 2.3		I 2.4.2,
Dänemark	III 2.3.6		I 2.4.5,
Frankreich	I 2.3.3		I 2.4.7
	II 2.3.4		II 4.1.1,
			II 4.1.1.1 e
Großbritannien, Kanada	I 2.3.2		III 1.4
	II 2.3.2,	Anpassung des —	III 1.5
	II 2.3.3		IV 1.5,
	III 2.3.1.2		IV 5.1.1
Neuseeland	III 2.3.1.9	— und Bundesgesetzgebung	I 4.1.1.2,
Österreich	III 2.3.7		I 4.1.3
Schweden	II 2.3.5		III 2.2.1
	III 2.3.5	Geltungsbereich des —	I 3.2,
Schweiz	III 2.3.8		I 4.1.1.3 d
USA	I 2.3.1,		II 4.1.1.3
	I 2.4.2,		III 1.5.1,
	I 2.4.5,		III 5.1
	I 2.4.7	US-von 1974	IV 2.2.3
	II 2.3.1		
	III 2.3.1	Datenschutzgesetzgebung	
Datenverarbeitung ohne —	I 1.2.3,	Tendenzen der —	I 2.4
	I 4.1.1.3 e		II 2.4
Notwendigkeit und Problematik des —	I 1.2.3		III 2.4
	II 1.3,	Datenschutzkommission	II 2.1.1
	II 1.3.1,	Datenschutzmaßnahmen	
	II 2.4		
Regelung des —	I 1.2.3	Differenzierung der —	II 2.4.1
Überwachung des —	I 2.4.7	Datenschutzpraxis	III 1.5.7
Instrumente des —	II 2.4,		IV 1.
	II 4.1.2.3	Datenschutz-Technologie	III 1.3
	IV 1.5.1	Datenschutzvorschriften	
Inhalt des —	II 4.1.2.1	Anwendungsbereich der — (Privater	I 2.4.1
— in der privaten Wirtschaft	II 1.3	Bereich, Öffentlicher Bereich)	II 2.4.1
Mindestanforderung für — und	II 4.3.1	— im Krankenhausgesetz	II 4.1.3.2
Datensicherung	III 4.3.1		III 4.1.1.1
Datenschutzbeauftragter		Datensicherung	I 1.1,
Unabhängigkeit des —	I 1.4		I 4.3,
	II 1.1,		I 5.8
	II 1.4		II 4.3
	III 1.4		III 4.3
Kontakt des —	II 1.4		IV 3.2
	III 1.3	— außerhalb des hessischen	I 4.3.2
— und private Unternehmen	II 4.1.1.3 d,	Datenverarbeitungsverbundes	II 4.3.2
	II 4.1.3.1,		III 4.3.2
	II 4.1.3.2	— im Einwohnerwesen	I 4.3.2
	III 1.5.1		III 4.1.3

—im hessischen Datenverarbeitungsverbund	I 4.3.1	EDV im Gesundheitsamt	III 4.1.1.3
	II 4.1.1.3,	EDV-Ausschuß des Landtags	IV 1.1
	II 4.3	Ehescheidungsakten	II 4.1.1.1 b
	III 4.3.1	Einführungsgesetz z. StGB	III 2.2.3
— Weiterentwicklung von Kontrollverfahren	III 4.3.3	Eingaben an den DSB	I 4.1.4
Regelung der —	I 1.2.3		II 4.1.4
Datensicherheit			III 1.3
Richtlinien für —	II 5.4	Einwohnerinformationssystem	IV 1.6
	III 4.3.1		I 2.2.1
Datenverarbeitung			III 4.1.3
— als Hilfsmittel der Verwaltung	I 1.4.2	Einwohnerwesen	II 3.1
	II 1.1		III 4.1.3
	III 3.		IV 1.5.2,
			IV 4.4
—im Gesundheitsamt	III 4.1.1.3	Elternrecht	IV 4.7.3,
Ergebnisse der —	I 1.3.2		IV 4.7.5
—im Statistischen Landesamt	I 4.1.1.3 b	Enquête-Kommission	
—in der HZD und den KGRZ	I 4.1.1.3 a	Zwischenbericht der —	
—in der öffentlichen Verwaltung	I 3.	BT-Drucks. VI/3829	II 2.4.2
	II 1.3	Entscheidungshilfe	II 4.2.3
integrierte —	I 1.2.2	Erfahrungsvorsprung des Landes gegenüber den Kommunen	II 4.2.4
	II 4.1.4,	Erfassung	IV 3.1
	II 4.1.1.1 c	Mehrfach- von Daten	I 3.1
konventionelle —	I 2.4.1		III 1.5.2
maschinelle —	I 1.2.2,	Erkennungsdienstliche Unterlagen	III 4.1.5.1
	I 1.2.3,	Europarat	IV 2.2.1
	I 1.3.2	Europäische Gemeinschaften	IV 2.2.1
	II 1.1,	Exekutive	I 1.2.2
	II 1.3		III 4.2.1
— ohne Datenschutz	I 1.2.3	Exekutivkompetenz	IV 4.3
Tendenz der — zur Zentralisierung	I 4.2.2		
Unterausschuß für —	II 5.1		
Datenverarbeitungsanlagen	II 1.1	Fairneß-Kodex	IV 1.2
Datenverarbeitungssysteme		Fernabruf	II 4.1.1.1
integrierte —	II 1.1	Fernübertragung	
	III 1.3	Daten —	I 4.1.1.1
Datenverarbeitungsverbund			III 2.5
Koordinierungsausschuß des hessischen —	I 4.2.2,	Finanzwesen	II 3.1
	I 4.3.1		IV 3.
Hessischer —	II 4.1.1.3 c	Forschungsauftrag	I 5.1.2
	II 4.1.1.3		III 5.9
	IV 4.2,	Forschungstests an Schulen	IV 4.7.5
	IV 5.1.2	Freiwilligkeit der Auskunft	III 4.1
im Krankenhauswesen	II 4.1.2.1,		IV 4.7.5
	II 4.1.3.2,		IV Anl. I
	II 4.3.2	Funktion	
— Krankentransport	III 4.1.1.2	-trennung	II 4.3.1
Datenverkehrsordnung	IV 1.2,	-verlagerung	II 4.2.2
	IV 1.5,		
	IV 1.5.1,	Gasölverwendungsgesetz	I 4.1.1.3 e
	IV 2.2.1,	Gebietsreform	II 4.2.2
	IV 4.7	Gefahrenabwehr	I 1.4.2
Datenweitergabeverbot	III 5.2		II 2.4.3,
Demokratische Prinzipien	I 1.2.1		II 2.4.4,
DEVO	II 4.1.1.2		II 2.4.5
DOMINIG	III 4.1.1.3		IV 1.5.3,
DÜVO	II 4.1.1.2		IV 4.1

Geheimhaltungs-		Analysesystem	I 4.2.4
-bestimmungen	I 1.2.1		II 4.2.3,
	III 2.2.1		II 4.2.4
	IV 4.6		IV 5.1.2,
-vorschriften	I 1.2.3		IV 5.2
-pflicht	II 2.2.4	- Kommunal	II 4.2.4
	III 4.2.1		IV 5.2
Geheimnischarakter von Merkmalen	I 1.2.3	Hessische Zentrale für Datenverarbeitung (HZD)	I 3.1,
Geltungsbereich des DSGVO	III 1.5.1		I 3.2,
Gemeindeplanungsdatei	II 4.2.4		I 4.1.1.3,
Generalklauseln			I 4.1.2,
Konkretisierung der —	II 4.1.2.1		I 4.2.2,
Genscher, Bundesminister	II 4.1.1.1 c,		I 4.2.4,
	II 4.1.1.3 b		I 4.3.1
			II 4.3.1
Gesetz über die Errichtung der Hessischen Zentrale für Datenverarbeitung und Kommunaler Gebietsrechenzentren (DVG)	I 1.2.2,		III 4.1.1.2,
	I 1.3.1		III 4.1.4
	IV 1.5.2	Hochschulstatistikgesetz	IV 4.2
Gesundheits-			I 4.1.1.2
-amt	III 4.1.1.3		
	IV 4.7.2		
-informationssystem	III 2.4,		
	III 4.1.1.3		
	IV 4.7.2		
-wesen	III 4.1.1.3		
	IV 1.5.2,		
	IV 2.2.1,		
	IV 2.3.3,	Identifizierungsmerkmale	I 1.2.3,
	IV 5.		I 4.1.1,
			I 4.1.1.1,
Gewaltenteilung			I 4.1.1.2,
Auswirkungen von Planungs- und Entscheidungshilfen der Regierung auf die —	I 4.2.1		I 4.1.1.3 b,
Erhaltung der —	I 4.2	getrennte Aufbewahrung der —	I 5.1
	III 4.2		I 5.2
			III 1.5.1 b
Unterstützung der Funktionen der —	I 2.4.1	Individualdaten	IV 3.1,
	III 4.2.1		IV 4.7,
			IV 4.7.7
Verschiebung in der —	I 1.4.1,	Statistik ohne —	I 5.3
	I 2.4.2		III 4.1.4
	IV 2.2.3	Individualinformation	I 1.2.1
Graduiertenförderungsgesetz	I 4.1.1.2	Schutz vor Mißbrauch der —	I 1.4
Grundrechte	I 1.2.1	Information(s)-	
		empfindliche —	I 5.2
			III 4.1.2
		-netz	I 2.4.3
Hamburg, Datenschutz in —	I 2.1.7,		III 1.3,
	I 2.2.2,		III 4.1.1.3,
	I 2.4.1		III 4.1.2,
Hard- und Software	III 1.3,		III 4.1.3
	III 4.3.1	-qualität	I 1.2.3
HEPAS (siehe Hess. Planungsinfor- mations- und Analysesystem)		-struktur	I 1.2.3,
			I 2.4.3
HEPOLIS	III 4.1.5.1	unbestätigte —	III 1.2.2
	IV 4.5.2	Informationsbankensystem	I 1.2.3
			IV 6.
„Hessen '80 — Datenverarbeitung“	I 1.2.2	— des Bundes	I 4.1.1.1
Hessischer Gemeindetag	II 4.1.1.3 d	Informationsbedürfnis	I 1.2.3
Hessisches			IV 1.5.2
— Beamten-gesetz (HBG, § 75)	II 4.1.1.1	Informationsfluß	I 1.2.1
— Planungs-informations- und	I 4.2.3,	Informationsgespräche	IV 1.4

Informationsgleichgewicht	I 1.2.2	Schutz der —	II 2.2.1
	II 2.4.2	IPEKS	II 2.1.3
	III 1.3,		
	III 4.2		
	IV 1.5.2,		
	IV 2.2.1,		
	IV 2.2.3,	Johanniter Unfallhilfe	III 4.1.1.2
	IV 5.,	Jugendgesundheitskarte	III 4.1.1.3
	IV 5.1.3,		IV 4.7.2
	IV 5.1.5,		
IV 5.1.6			
Informationsmißbrauch	I 1.2.3		
	III 1.2.2	Kamlah	I 1.2.3
Informationsrechte parlamentarische —	I 4.2.3	Katastrophenpläne	II 4.3.1
	II 4.2.3	Kirchen (s. auch Religionsgesellschaften)	I 4.1.1.3 f,
	III 4.2.1		I 4.1.2
	IV 5.	— und Datenschutz	IV 4.4
			II 4.1.1.1 b,
Informationsstruktur Eingriffe in die —	II 2.4.1		II 4.1.1.3 f,
			II 4.1.2.1
Informationssystem	I 1.2.3		III 1.3,
	IV 2.2.3		III 4.1.6
allgemeines — Einwohner-	I 1.2.3	Kirchensteuergesetz — hess.	II 4.1.1.3 f
	I 1.2.3	Kommission der EG	III 2.5
Gesundheits- integriertes —	III 4.1.1.3	Kommunale	
	I 1.2.1,	— Spitzenverbände	II 4.2.2
parlamentarisches —	I 1.2.2,	— Vertretungsorgane	I 1.3.1
	I 1.2.3	Kommunales Gebiets-Rechen-Zentrum (KGRZ)	I 3.1,
Personal- polizeiliches —	I 4.2.1		I 3.2,
	III 4.2.1,		I 4.1.1.3,
— bei Verfassungsschutz	III 4.2.2		I 4.1.2,
	III 4.1.2		I 4.2.2
Informationsverbund	I 4.1.1.3 c		II 4.3.1
	II 4.1.1.3 c		III 1.5.6
Informationsweitergabe dysfunktionale —	III 4.1.5	Kommunen	IV 4.2
	IV 1.5.2,		IV 2.2.3,
Infrastruktureinrichtungen Planungsdatei für —	IV 4.5,		IV 3.1,
	IV 4.5.2		IV 4.2.3,
Inkompatibilität — bei Übertragung der Datenschutz- kontrolle auf Bundesminister	IV 2.2.3,		IV 4.3,
	IV 4.5		IV 4.4,
INPOL	III 4.1.1.3	Einfluß der EDV auf Verhältnis der — zum Land	IV 5.1.4
	II 4.1.2.2	Erhöhung der Verwaltungskraft der — Kontrolle	I 4.2.2
Integration	II 4.2.4		II 2.4.3
	I 1.4.2		III 1.4,
Internationales Zusammenwirken	I 2.4.7		III 1.5.2,
	III 4.1.5.1		III 2.2.1
Intimsphäre	IV 4.5		III 2.2.2,
	I 1.2.2		III 2.4,
— bei Verfassungsschutz	III 1.3		III 4.2.1,
	I 2.3	demokratische —	III 4.3.5
Informationsverbund	II 2.3	externe —	IV 1.5.2,
	III 2.3		IV 3.2
Informationsweitergabe dysfunktionale —	IV 1.3.4		IV 2.1,
	I 1.2.3,		IV 2.2.1,
Infrastruktureinrichtungen Planungsdatei für —	I 4.1.1.3 c,	Kontrollverfahren	IV 2.2.3
	I 4.1.2,	Weiterentwicklungen von —	
Inkompatibilität — bei Übertragung der Datenschutz- kontrolle auf Bundesminister	I 5.4	Kooperationsausschuß ADV Bund/Länder/ Gemeinden	III 4.3.3
	III 4.1		III 1.2,
			III 2.5

Koordinierungsausschuß		Wahl des DSB durch den—	I 1.4
— des hess. Datenverbundes	II 4.1.1.3 a	Legislative	I 1.2.2
	III 4.3.1		III 4.2.2
— Hess. Statistischer	II 4.1.1.3 b	Lehrerdatei	III 4.1.2
Kostenfreiheit	II 4.2.2	Lehrstuhl	III 1.5.7
Krankenhausgesetz	II 4.1.2.3	Leistungssport	III 4.1.1.3
	III 1.5.3,	Löschung von Daten	II 4.1.1.3 c,
	III 4.1.1.1		II 4.1.1.3 e
	IV 1.5.2		III 4.1.7
Krankenhauswesen	III 2.4,		IV 1.5.1,
	III 4.1.1.1		IV 4.3,
Krankentransport	III 4.1.1.2		IV 4.7.2
Krankenversicherung	II 4.1.1.2	Machtbalance zwischen Parlament und	
Kriminalpolizei	II 1.1	Regierung	I 1.4
Informationssystem der—	II 2.4.3	Malteser-Hilfsdienst	III 4.1.1.2
	III 4.1.5.1	Maschinenkapazität	III 3.
	IV 1.5.2,	Massachusetts	III 2.3.1.1
	IV 2.2.3,	medizinische Daten	II 4.1.2.3
	IV 4.5,		III 4.1.1,
	IV 4.5.1,		III 5.5
	IV 4.5.2	medizinische Datenbanken	III 4.1.1.3
— Zusammenarbeit mit privaten			IV 4.7.2
Unternehmen	II 4.1.1.3 d	Meldewesen	I 2.2.1
		Mikrozensus (s. Bundesverfassungsgericht)	III 4.1.3
Landesamt für Verfassungsschutz	II 4.1.1.3 e,	Mißbrauch von Informationen	II 4.1.1.1 c
	II 4.1.2.1		IV 1.4
	III 4.1.5.1	Müller, Paul J.	II 4.1.2.2
	IV 4.5		
Landeskriminalamt	I 1.2.3,	Nachrichtendienste	
	I 4.1.1.3 c	Informationssysteme der—(NADIS)	II 1.1,
	II 4.1.1.3 c,		II 2.4.3,
	II 4.1.1.3 d,		II 4.1.1.3 e
	II 4.1.2.1		III 4.1.5.2
	IV 4.5.1,		IV 2.2.3,
	IV 4.5.2		IV 4.4
Landesregierung	I 1.1,	Niedersachsen, Datenschutz in—	I 2.1.4
	I 1.2.2,		III 2.1.4
	I 1.3.1	Nordrhein-Westfalen, Datenschutz in—	I 2.1.6
	III 4.1.5.1,		I 2.2.2,
	III 4.2.1		I 2.4.1,
	IV 4.1		I 2.4.2
Landesverwaltung	I 1.2.2		III 1.3,
	II 4.1.1.3		III 2.1.6
Ausführung der Bundesgesetze		Normfindung	III 1.5.7,
durch die—	I 4.1.1.2		III 6.
Kontrolle der— durch DSB	I 4.1.1.2		IV 1.5,
	II 4.2.3		IV 2.2.3
	III 1.5.1,	OECD	III 2.5
	III 4.2.2		IV 2.2.1
Landtag		Operatives Handeln	I 2.1
Arbeitsgruppe EDV des—	III 4.2		
	IV 1.1	Parlamente	
Informationsrecht des—	I 1.3.1	Auskunftersuchen der—	I 1.4.1
	II 4.2.3		III 4.2.1
	III 4.2.1,		
	III 4.2.2	Herausforderung der— durch Einsatz	
	IV 5.1,	der EDV	I 4.2.1
	IV 5.1.1	Informationsrechte der—	I 2.4.1
Unterausschuß des— für EDV	II 5.1		III 4.2.1

— und Informationssysteme	I 5.9	Eingriffe in das — in der Bundesgesetzgebung	I 4.1.1.2
	II 4.2.4		
— und Regierung	I 4.2.1	Gefährdung des —	II 4.1.1.1 c
	IV 4.1	Schutz des —	I 4.1,
— und statistische Veröffentlichungen	III 4.2.3		I 4.1.1.1
Personalakten			II 4.1,
Einsicht in —	II 2.4		II 4.1.1.1 c
	III 1.2.1		III 4.1
Personalwesen	II 3.1	Persönlichkeitsschutz	IV 1.5.1
	IV 3.		I 1.4,
Personaldatenbanken	III 4.1.2		I 2.4.1
	IV 1.4		II 2.4.2
Personalstrukturdatei	III 4.1.2	Planerisches Handeln	I 1.2.1
Personenbezogene Daten	I 1.2.3,	Planung	
	I 3.1,	—bürokratie	I 4.2.1
	I 4.1.1,	— und Entscheidungshilfe	I 4.2.1
	I 4.1.2		IV 5.1.3
	II 3.1	integrierte —	I 4.2.1
	IV 1.4,		IV 5.1.3
	IV 1.5.3,	kommunale —	II 4.2.4
	IV 1.6,		
	IV 1.7,	Planungsinformation	
	IV 2.2.2,	politische —	II 4.2.4
	IV 2.2.3,	Polizei-Informations-System	III 4.1.5.1
	IV 3.1,		IV 1.5.2,
	IV 4.5,		IV 2.2.3,
	IV 4.7,		IV 4.5,
	IV 4.7.7		IV 4.5.2
Erhebung —	I 4.1.1.1,	Podlech, A.	II 4.1.1.1
	I 4.1.1.2		III 2.2.1
Ermittlung —	III 1.5.2		
—in der Landesverwaltung	I 4.1.1.3	Praxis	
—in der Bundesgesetzgebung	I 4.1.1.2	Wissenschaft und —	III 1.5.7
Umgang mit —	I 4.1.1		IV 1.5
	II 4.1.1	Private Unternehmen	I 1.3.2
	III 1.3,		II 4.1.3
	III 1.5.1,		III 1.5.1
	III 1.5.5,		IV 2.2.3
	III 1.5.6	Hilfe durch — bei Verwaltungsaufgaben	I 4.1.2.3 d
Weitergabe —	III 4.1,		II 4.1.1.3 d,
	III 1.5.6,		II 4.1.3.1,
	III 5.2		II 4.1.3.2
	IV 3.1	Zusammenarbeit mit —	II 5.2
Personalinformationssystem	III 4.1.3		III 5.1
Personenkennzeichen	I 2.2.1	Privatrecht	
	III 4.1	Regelung im Bereich des —	I 1.3.2
Persönlichkeitsprofil	II 1.3.2,	Privatsphäre	I 1.2.1,
	II 4.1.1.1 c		I 1.2.3,
Persönlichkeitsrecht	I 1.2.3		I 1.3.1
	III 1.5,		III 4.1
	III 4.1,		IV 1.6,
	III 5.5		IV 2.2.1,
	IV 1.4,		IV 4.7.7
	IV 1.5.1,	Beschränkungen der Datenschutzvorschriften auf den Schutz der —	I 2.4.2
	IV 1.5.3,	Eindringen in die —	I 4.1.1.2,
	IV 2.2.3,		I 4.1.1.3 c
	IV 4.6,	Schutz der — im Verhältnis zur Kirche	I 4.1.1.3 f
	IV 4.7,		III 4.1.6
	IV 4.7.5,	Interpretation der —	II 4.1.2.2
	IV 4.7.8,		
	IV 6.		

Programme für Datenschutz	II 1.3.1	Sicherheitsbestimmungen	I 1.2.1
	III 4.3.1		II 4.3.1
Programm-Manipulation	III 4.3.1,	Simitis, Sp.	I 1.2.3
	III 4.3.3		III 2.2.1
Protokolle über Datenabruf	I 2.2.1	Sozialarbeiterin	III 1.2.1
	III 4.1.3 a	Sozialversicherungen und Datenschutz	I 4.1.1.3 d
Protokollierung			II 4.1.1.2
automatische —	I 2.4.4	Sparkassen- und Giroverband	III 1.5.1
	II 2.4.3,	Sperren	IV 1.5.1
	III 2.4.4,	— gegen Abruf	I 2.2.1
	II 2.4.5		III 4.3.3
	III 4.3.1,	— gegen Privatauskünfte	I 2.2.1
	III 4.3.3	Sphärentheorie	I 1.2.3
	IV 1.5.1,		II 4.1.2.1
	IV 3.2	Staatsgerichtshof — Urteil vom 27. 10. 65 —	I 4.1.1.3 f
Prüf- und Analyseprogramme	III 4.3.3	Stadtplanung	III 1.5.1 c
		Statistik	I 4.1.1.1
Rationalisierung der Verwaltung	I 1.2.2		III 4.2.3
Rechnungshof für das Land Hessen	II 4.3.1		IV 3.2,
Religionsgesellschaften			IV 5.1.3
öffentlich-rechtliche —	II 2.2.1	Bundes-	I 4.1.1.2
	II 4.1.1.3 g		IV 4.6
Rentenauskunftsverfahren	II 4.1.1.3 g	— ohne Individualdaten	I 5.4
Rentenversicherung	II 4.1.1.2	gesetzliche Verankerung der —	II 4.1.1.3 b
Rheinland-Pfalz, Datenschutz in —	I 2.1.3,	Scheidungs-	I 4.1.2
	I 2.4.2	Statistisches Bundesamt	I 4.1.1.1,
	II 2.1.3		I 4.1.2
	III 1.3,	Statistisches Landesamt	I 4.1.1.3,
	III 2.1.3		I 4.1.2
Einwohnerinformationssystem in —	I 1.2.3		II 4.1.1.3 b
Rotes Kreuz	III 4.1.1.2		III 4.1.4,
Rückidentifizierung	IV 1.7		III 4.2.3
			IV 4.4.6
Saarland, Datenschutz im —	I 2.1.8	Steinmüller, W.	I 1.2.3
Schleppnetz-Technik	IV 4.5.1	Strafvorschriften	I 2.2.4,
Schleswig-Holstein, Datenschutz in —	I 2.1.1		I 2.4.6
	II 2.1.1		II 2.2.4
Schülerdatei	III 4.1.2	Studentendateien	IV 4.7.3,
	IV 4.7.3		IV 4.7.4
Schulsportärztlicher Untersuchungsbogen	III 4.1.1.3		
	IV 4.7.1,	Tätigkeitsbericht	
	IV 4.7.2	parlamentarische Behandlung des —	II 1.1
Schutzmaßnahmen	II 4.3.2		III 4.2
Schweigegebot			IV 1.1,
			IV 4.1
Aufhebung des —	I 1.4	Testläufe	IV 4.7.7
Schweigepflicht		Tiedemann/Sasse	III 2.2.1
ärztliche —	II 4.1.2.3	Transparenz	II 2.4.3,
Seidel, U.	II 4.1.1.1		II 4.1.4
Selbstbestimmungsrecht	IV 4.7.8		
	IV Anl. I	Universitäten	III 4.3.2
Service-Unternehmen	I 1.3.2,	Universitätsklinik	III 1.5.7
	I 4.1.2.3 d	Unterlagen für die Zwecke der maschi-	I 1.3.2,
	II 4.1.1.3 d,	nellen Datenverarbeitung	I 3.2
	II 4.1.3.1,	Unterlassungsanspruch des Bürgers	I 2.4.5
	II 4.1.3.2,	Unterrichtung des DSB	IV 4.7.6
	II 5.2	Untersuchungsbogen	III 4.1.1.3
	III 5.1	Urmaterial der Erfassung	I 4.1.1.1
	IV 4.3		

Verantwortung für Datenschutz	I 5.6	Volkvertretung	
	II 4.1.1.3 dm,	kommunale—	II 4.2.4
	II 4.1.3.2	Initiativfunktion und Kontrollfunktion der—	II 4.2.4
Verfahrensentwicklung	IV 4.3	Vorschlagswettbewerb	III 1.5.8, III 5.7
Prioritätensetzung bei der—	II 4.2.2		II 4.1.1.1 c
Verfassungsschutz	III 4.1.5.2	Wahlrechtskartei	I 2.4.2
Verkehrsordnungswidrigkeiten	II 4.2.2	Westin, Alan F.	I 2.4.5
Verkehrsplanung	III 1.5.1 b	Wiederherstellungsanspruch des Bürgers	
Verkehrsverbund	III 1.5.1 b	Wissenschaft und Praxis	III 1.5.8
Verpflichtungsgesetz	III 2.2.3	Zusammenarbeit von—	IV 1.5
Verrechtlichung von Verwaltungsvorschriften	II 4.1.1.3 c, II 4.1.1.3 e, II 5.3 III 1.5.4, III 5.4 IV 4.5, IV 4.5.1	Wohngeld Auszahlung des— mittels EDV -daten Wohnungsstichprobengesetz Entwurf eines—	I 4.1.1.3 d II 4.2.3 I 4.1.1.2
Verschwiegenheitspflicht	I 1.4, I 4.1.1.1, I 4.1.2 II 4.1.1.1	Zielkonflikt Datenschutz-Datenverarbeitung Zugang zu Daten Zugriff auf Datenbestände	II 2.4.3 I 4.2.2 I 1.2.3, I 4.1.2, I 5.4 IV 1.5.2
Verschwiegenheitsvorschriften	I 1.2.3		
Versicherungsvertreter	III 1.2.1		
Vertraulichkeit der Angaben des Bürgers	I 4.1.1.1 II 4.1.1.1 c, II 4.1.2.2, II 4.1.2.3	Zugriffsrecht	I 1.2.3 III 1.5.6 IV 5.1.4, IV 5.1.5
Verwaltung		—des Parlaments	IV 5.1, IV 5.1.1, IV 5.1.5
öffentliche—	I 1.2.3, I 1.3.2, I 4.3 II 4.2.2 III 1.5.1	Zusammenarbeit der Verwaltung und privater Stellen	I 4.1.1.3 dm, I 5.5 II 4.1.1.3 d IV 4.7.8
-aufbau	II 4.2.2		
-verfahren	II 4.2.2		