HESSISCHER LANDTAG

8. Wahlperiode

Drucksache **8/3962**

11. 03. 77

Sechster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

Mit Schreiben vom 10. März 1977 legt der Datenschutzbeauftragte gemäß § 14 Abs. 1 des Datenschutzgesetzes vom 7. Oktober 1970 dem Landtag den folgenden Tätigkeitsbericht vor:

Eingegangen am 11. März 1977 · Ausgegeben am 9. Mai 1977

Druck: Carl Ritter & Co., Wiesbaden · Vertrieb: Verlag Dr. H. Heger, Goethestr. 56, 53 BN-Bad Godesberg, Tel. (02221)/363551

INHALTSVERZEICHNIS

Die fünf vorangegangenen Tätigkeitsberichte werden bei Hinweisen mit I, II, III, IV und V benannt. Die nachfolgenden arabischen Ziffern bezeichnen den Abschnitt in dem entsprechenden Tätigkeitsbericht.

1. EINLEITUNG

1. **Einleitung**

Der im März 1976 vorgelegte Fünfte Tätigkeitsbericht des Hessischen Datenschutzbeauftragten hatte sich bereits eingehend mit den möglichen Konsequenzen eines Bundesdatenschutzgesetzes beschäftigt. Bei diesen ersten Überlegungen kann es nicht bleiben. Das Bundesdatenschutzgesetz ist mittlerweile verabschiedet, das Landesdatenschutzgesetz soll folgen. Der Schwerpunkt des Sechsten Tätigkeitsberichts ergibt sich insofern fast von selbst: Es gilt, die Erfahrungen aus der bisherigen Anwendung des Hessischen Datenschutzgesetzes ebenso zu nutzen wie die lange Diskussion über das Bundesdatenschutzgesetz, um dem Hessischen Landtag einen Gesetzesvorschlag zu unterbreiten. Dem Parlament soll damit ermöglicht werden, möglichst schnell eine Entscheidung zu treffen und damit den Bürger nicht zuletzt vor den Nachteilen zu bewahren, die sich aus unterschiedlichen Ansatzpunkten des noch geltenden Landesrechts und des neuen Bundesrechts ergeben könnten.

1.1 So sehr es aber darauf ankommt, eine Regelung zu finden, die ein Höchstmaß an Datenschutz gewährleistet, so wenig lassen sich die Grenzen übersehen, die aus der Existenz des Bundesdatenschutzgesetzes folgen. Im Interesse des Bürgers kommt es darauf an, eine Zersplitterung des Datenschutzes zu verhindern. Der Preis dafür ist der Verzicht auf jenen Weg, der für den hessischen Gesetzgeber 1970 noch gangbar war: Eine Gesetzgebung, die deshalb die jeweils überzeugendste Lösung aufnehmen kann, weil sie nicht mit Rücksicht auf andere schon bestehende Regelungen zu Konzessionen bereit sein muß. Einheitlichkeit des Datenschutzes kann und darf aber nicht schlicht Übernahme des Bundesdatenschutzgesetzes auf Landesebene bedeuten.

Der Bundesgesetzgeber selbst hat in § 7 BDSG die zentrale Rolle der Landesdatenschutzgesetze für die weitere Entwicklung des Datenschutzes ausdrücklich anerkannt. Der hessische Gesetzgeber hat allen Grund, diese Chance wahrzunehmen, schon mit Rücksicht auf die Erfahrungen mit dem eigenen Gesetz. Abgesehen davon aber hat die Landesgesetzgebung in diesem Bereich von Anfang an noch ein weiteres Ziel verfolgt: Sie will nicht nur den Respekt vor der Person des einzelnen sicherstellen, sondern auch das Informationsgleichgewicht gewährleisten. Diese zusätzliche Aufgabe muß nach wie vor ebenfalls im Mittelpunkt des Landesdatenschutzgesetzes stehen.

1.2 Weder das Bundes- noch das Landesdatenschutzgesetz genügen freilich, um die sich aus der Verfassung ergebende Pflicht des Gesetzgebers zum Schutz der persönlichen Integrität des Bürgers zu erfüllen. Mehr denn je macht sich vielmehr die Notwendigkeit bemerkbar, den allgemeinen Datenschutz durch eine Reihe spezieller Regelungen für einzelne, gerade aus der Perspektive des Bürgers besonders wichtige, Bereiche zu ergänzen. Die Verarbeitung personenbezogener Daten durch die Polizei, den Verfassungsschutz sowie im Rahmen des Gesundheitswesens sind Beispiele, die bereits in den vergangenen Tätigkeitsberichten mehrfach angesprochen worden sind. Die Erfahrungen mit dem Krankenhaus- und dem Melderecht sollte nicht vergessen werden. Ohne eine Berücksichtigung der sich aus dem Datenschutz ergebenden Forderung kann es eine überzeugende, den Grundsätzen der Verfassung entsprechenden Regelung in keinem dieser Bereiche geben. Ich erwähne dies nicht zuletzt im Hinblick auf den Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder. In die Diskussion über ein solches Gesetz müssen von Anfang an Überlegungen zum Datenschutz einbezogen werden. Auch hier befindet sich das Land Hessen in einer besonders glücklichen Lage. Es liegen Richtlinien vor, die durchaus die Möglichkeit bieten, die aus der Perspektive des Datenschutzes erforderlichen Konsequenzen zu ziehen. Der Zeitpunkt ist gekommen, an dem die in diesen Richtlinien enthaltenen Ansatzpunkte aufgegriffen und weiterentwickelt werden müssen. Dies umso mehr, als es nicht im Interesse des Bürgers liegen kann, wenn der Datenschutz im polizeilichen Bereich lediglich in einem einzigen Land in der Bundesrepublik speziell geregelt ist.

1.3 Die hessischen Erfahrungen haben auch im vergangenen Jahr die internationale Diskussion über den Datenschutz maßgeblich beeinflußt. Als Beispiel seien die Anhörung des Hessischen Datenschutzbeauftragten durch die Britische Kommission, seine intensive Beteiligung an den Arbeiten des Europarats und der OECD sowie seine Teilnahme an der Diskussion über den französischen Gesetzentwurf genannt.

Wie in jedem Jahr enthält der Bericht einen Überblick über die wichtigsten ausländischen Entwick-

lungen. Sie zeigen, daß die Zahl konkreter Vorschläge für eine Datenschutzregelung ständig zunimmt. Zugleich wird deutlich, wie wenig sich die Annahme rechtfertigen läßt, das Bundesdatenschutzgesetz stelle die einzige mögliche Lösung der Datenschutzprobleme dar. Im Gegenteil: Nach Schweden scheinen jetzt auch die Niederlande und Kanada eine Regelung anzustreben, in deren Mittelpunkt Registrierung und Konzessionierung der Datenbanken stehen. Die vom Europäischen Parlament unterstützten Bemühungen der Europäischen Gemeinschaft um eine möglichst einheitliche Regelung werden dadurch bestimmt nicht erleichtert.

Trotzdem bietet diese Unterschiedlichkeit einen nicht zu unterschätzenden Vorteil: Sie bewahrt den nationalen Gesetzgeber vor der Annahme, den Anforderungen des Datenschutzes mit seiner Regelung wirklich und endgültig entsprochen zu haben. Die unterschiedlichen Ansatzpunkte zwingen vielmehr dazu, Vor- und Nachteile der verschiedenen Regelungssysteme sorgfältig zu beobachten, und zwar im Hinblick auf eine kontinuierliche Verbesserung der eigenen Gesetzgebung.

Besondere Bedeutung kommt den Bemühungen des Europarats und der OECD zu. Mit Hilfe der von beiden Organisationen angestrebten Übereinkommen könnte es gelingen, die nationalen Bemühungen aufeinander abzustimmen, zugleich aber, wie sich am Beispiel der grenzüberschreitenden Datenverarbeitung erweist, Fragen zu regeln, die bislang im nationalen Bereich nicht überzeugend oder überhaupt nicht behandelt werden können.

1.4 Der Tätigkeitsbericht enthält schließlich eine Reihe konkreter Datenschutzfälle. Sie wurden vor allem unter einem Gesichtspunkt ausgewertet: In den Diskussionen über den Datenschutz spielt die Vorstellung noch immer eine wichtige Rolle, daß seine eigentliche Aufgabe darin besteht, gegenwärtigen „Mißbrauch" zu bekämpfen und zukünftigen zu vermeiden. Das Bundesdatenschutzgesetz scheint mit seinen einleitenden Formulierungen diese Annahme zu bestätigen. Jeder der im Tätigkeitsbericht angeführten Fälle zeigt freilich, wie mißverständlich solche Hinweise sind. Weder bei der Weitergabe personenbezogener Daten, die in Bauanträgen enthalten sind, noch bei der Verwendung von EDV-Unterlagen als Schmierpapier kann ernsthaft von einem „Mißbrauch" im Sinne eines konkret vorwerfbaren, weil beabsichtigten Verstoßes gegen die Grundsätze des Datenschutzes die Rede sein. Was sich vielmehr an den einzelnen Fällen immer wieder zeigt ist, wie sehr nach wie vor im Umgang mit personenbezogenen Daten das Bewußtsein der Notwendigkeit fehlt, die persönliche Integrität des Bürgers zu respektieren. Unstreitig nehmen die Fälle, in denen die Behörden mit dem Datenschutzbeauftragten eng zusammenarbeiten, ständig zu. Und ebensowenig läßt sich bestreiten, daß sehr viele Behörden von sich aus mittlerweile die Initiative ergreifen, um den Schutz des Bürgers zu verbessern. Dennoch ist der Datenschutz noch keineswegs zur Selbstverständlichkeit geworden. Er bleibt konkrete, tagtäglich zu verwirklichende Aufgabe.

2. VORSCHLAG FÜR EIN LANDESDATENSCHUTZGESETZ

2. Vorschlag für ein Landesdatenschutzgesetz

2.1 Im Fünften Tätigkeitsbericht (LT-Drucks. 8/2475) habe ich die Konsequenzen dargelegt, die sich für das Landesrecht und die Landesverwaltung ergeben würden, wenn ein Bundesdatenschutzgesetz idF des damals vorliegenden Entwurfs in Kraft träte. Aufgrund dieser Überlegungen habe ich empfohlen, das hessische Datenschutzgesetz (HDSG) alsbald zu novellieren. Inzwischen ist das Bundesdatenschutzgesetz vom 27. Januar 1977 (BDSG) verkündet worden; es tritt am 1. Januar 1978 in Kraft. Das BDSG enthält – abweichend vom Regierungsentwurf – einen Vorbehalt für die Landesgesetzgebung: Das Gesetz soll für die öffentliche Verwaltung der Länder, soweit sie Bundesrecht ausführen, und für ihre Rechtspflegeorgane im Bereich der Rechtsprechung nur gelten, soweit der Datenschutz nicht durch Landesgesetz geregelt ist (§ 7 Abs. 2 BDSG). Dieser Regelung liegt ein Vorschlag des Vermittlungsausschusses (Art. 77 Abs. 2 GG) zugrunde, der einer Initiative des Bundesrats folgt. Bundestag und Bundesrat haben dabei die Erwartung zum Ausdruck gebracht, daß die Länder übereinstimmende, dem Bundesgesetz angeglichene Datenschutzgesetze schaffen.

Die Ausformung einzelner Datenschutzregelungen des BDSG war im Gesetzgebungsverfahren hart umstritten; der Einigungsvorschlag des Vermittlungsausschusses ist sowohl im Bundestag als auch im Bundesrat nur mit der Mehrheit der Stimmen angenommen worden. Sieht man von einer Minderheit ab, die das Gesetz im ganzen abgelehnt hat, so bestand weitgehend Übereinstimmung darüber, daß das Bundesgesetz „verbesserungswürdig" ist[1]). Die Datenschutzgesetzgebung sei als ein kontinuierlicher Prozeß zu verstehen, Entwicklung und Verbesserung des Datenschutzrechtes blieben über das Gesetzgebungsvorhaben hinaus eine dauernde Aufgabe[2]).

Danach hat die Datenschutzgesetzgebung, zu der die Länder nunmehr aufgerufen sind, zwei verschiedenartigen Anforderungen zu genügen: Einerseits das Datenschutzrecht für die Landesgesetzgebung weiter entwickeln und Mängel des Bundesgesetzes beseitigen; andererseits die Bundeseinheitlichkeit des kodifizierten Datenschutzrechtes auf breiter Grundlage wahren.

Mit diesen Maßstäben sollte geprüft werden, ob und wieweit der Aufbau des BDSG sowie seine einzelnen Vorschriften in das Landesrecht unverändert übernommen werden können oder welche Verbesserungen anzubringen sind.

Der als Anlage beigefügte Text eines Gesetzentwurfes – im weiteren als „Entwurf" (E) bezeichnet – ist das Ergebnis meiner Untersuchung; er könnte ein Modell für übereinstimmende Landesgesetze sein.

2.2 Die Abweichungen vom BDSG beruhen auf den folgenden Erwägungen:

2.2.1 Die Gliederung des BDSG ist von der Aufteilung auf drei „Anwendungsbereiche" bestimmt, von denen der eine die Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen und die beiden anderen die Datenverarbeitung im nicht-öffentlichen, das heißt im Bereich privater Betätigung umfassen. Diese Aufteilung entfällt für das Landesgesetz. Das BDSG hat dem Landesgesetzgeber die Regelung des Datenschutzes nur für die Datenverarbeitung der Behörden und öffentlichen Stellen des Landes und dessen Rechtsprechungsorgane vorbehalten. Dieser Vorbehalt deckt auch die allgemeinen Vorschriften des ersten, fünften und sechsten Abschnitts des BDSG; denn die §§ 1 bis 6 sowie die Übergangs- und Schlußvorschriften des BDSG gelten nur, soweit die Regelung der drei Anwendungsbereiche gilt, wie sich aus § 1 Abs. 2 BDSG ergibt.

Abgesehen von den Vorschriften im dritten Abschnitt des Entwurfs (Informationsgleichgewicht) folgt daraus für das Landesgesetz die Gliederung in: Allgemeine Vorschriften, Vorschriften für die Datenverarbeitung, Vorschriften für den Datenschutzbeauftragten und Schlußvorschriften.

2.2.2 Der Datenschutz hat im geltenden Landesrecht zwei Aufgaben:

1. den einzelnen davor zu schützen, daß seine grundrechtlich verbürgte Rechtsstellung gegenüber dem Staat durch die behördliche Datenverarbeitung beeinträchtigt wird;
2. das verfassungsmäßige Gefüge des Staates – und entsprechend der kommunalen Vertre-

[1]) Dr. Hirsch, NW, Bericht über die 440. Sitzung des Bundesrates am 12. 11. 1976, S. 411 (C).

[2]) Dr. Günther, 436. Sitzung des Bundesrates am 25. 6. 1976, S. 296 (D).

tungskörperschaften –, das auf dem Prinzip der Gewaltenteilung beruht, vor nicht verfassungskonformen Veränderungen infolge der Datenverarbeitung zu bewahren, mit anderen Worten: Das „Informationsgleichgewicht" zu erhalten oder wieder herzustellen.

Daß das BDSG die letztgenannte Aufgabe nicht aufgegriffen hat, steht der Fortgeltung der landesrechtlichen Regelung und ihrer Weiterentwicklung nicht entgegen.

2.2.2.1 Die Definition der Aufgabe des Datenschutzes hat keinen unmittelbaren Regelungsgehalt; sie hat mehr den Charakter eines Vorspruchs (Präambel), der, wie es in der Regierungsvorlage zum BDSG noch hieß, den „Zweck des Gesetzes" und die Motivation des Gesetzgebers offenlegen soll. Daher wird die wörtliche Übernahme des § 1 Abs. 1 BDSG nicht empfohlen. Was „Mißbrauch" im Sinne des Gesetzes ist, folgt allein aus den einzelnen Regelungen über die Zulässigkeit der Datenverarbeitung. Die „schutzwürdigen Belange" sollen nach der Begründung der Regierungsvorlage die aus der Würde des Menschen und seiner Handlungsfreiheit (Art. 1 Abs. 1 und Art. 2 Abs. 1 GG) abgeleitete Grundrechtsposition des einzelnen, sein „Persönlichkeitsrecht", bezeichnen. Da der einfache Gesetzgeber Umfang und Schranken von Grundrechten nur Kraft – hier fehlender – verfassungsrechtlicher Ermächtigung näher bestimmen kann, ist der Begriff „schutzwürdige Belange" eine kaum definierbare Floskel, die das Verständnis der Vorschrift nur erschwert.

2.2.2.2 Der hessische Gesetzgeber hat die Bewahrung des Gewaltenteilungsprinzips vor Veränderungen durch die Datenverarbeitung als eine Funktion des Datenschutzes und nicht als eine „weitere" Aufgabe des Datenschutzbeauftragten verstanden wissen wollen. Deswegen wird in **§ 1 Nr. 2 E** die in § 10 Abs. 2 HDSG umschriebene Aufgabe des Datenschutzbeauftragten in einer einfacheren Formulierung als Zweck und Inhalt des Datenschutzes herausgestellt.

2.2.2.3 § 1 Abs. 2 BDSG umschreibt den Geltungsbereich des Bundesgesetzes in den drei Anwendungsbereichen. Für das Landesgesetz hat diese Vorschrift nur im Rahmen der Subsidiaritätsklausel des § 7 Abs. 2 BDSG Bedeutung. Sie kehrt daher in **§ 2 E** als Vorschrift über den Geltungsbereich des Landesgesetzes wieder.

2.3 Das BDSG gilt – mit Ausnahme des § 6 – nicht für personenbezogene Daten, die weder zur Übermittlung an Dritte bestimmt sind, noch in automatisierten Verfahren verarbeitet werden. Für den öffentlichen Bereich des Landes halte ich diese Einschränkung des Datenschutzes nicht für gerechtfertigt.

Die Regelung des Bundesgesetzes entspricht dem Antrag des Bundesrates im Vermittlungsverfahren. Sie ist ein Kompromiß zwischen der Regierungsvorlage, die nicht zur Übermittlung bestimmte Daten aus dem Datenschutz herausnahm, und der Empfehlung des Bundesrates im ersten Durchgang, die einen möglichst lückenlosen Datenschutz anstrebte. Die Gesetz gewordene Zwischenlösung trägt den Bedenken Rechnung, die vor allem von Wirtschaftsverbänden für den nicht-öffentlichen Anwendungsbereich des BDSG erhoben worden waren.

Im übrigen ist die bloße Verweisung auf § 6 BDSG, der als einzige Vorschrift für die oben bezeichneten Daten gelten soll, nicht vollziehbar, weil sie in sich widersprüchlich ist.

2.4.1 Dem Staat, den seiner Aufsicht unterstellten juristischen Personen des öffentlichen Rechts sowie den Gemeinden und Gemeindeverbänden soll, soweit sie sich mit selbständigen oder unselbständigen **Unternehmen** – die Begründung zu § 5 Abs. 2 der Regierungsvorlage des BDSG spricht von „öffentlichen Stellen" – **am Wettbewerb** beteiligen, keine Sonderstellung eingeräumt werden. Dies entspricht § 7 Abs. 1 und 2 BDSG.

Für den Landesgesetzgeber stellt sich aber die Frage, ob er es dabei bewenden lassen kann, die Geltung wesentlicher Teile seines Gesetzes für diese öffentlich-rechtlichen Wettbewerbungsunternehmen auszuschließen, oder ob er darüber hinaus bestimmen muß, welchen Datenschutzvorschriften diese Unternehmen unterworfen sein sollen. Das hängt davon ab, ob die Vorschriften im dritten und vierten Abschnitt des BDSG ausreichen, um die bezweckte Gleichstellung mit den vergleichbaren privatrechtlichen Unternehmen zu erreichen; das ist zweifelhaft:

Nach § 22 Abs. 1 und § 31 Abs. 1 BDSG gelten für die am Wettbewerb teilnehmenden öffentlichrechtlichen Unternehmen die Vorschriften des dritten oder vierten Abschnittes des BDSG jeweils mit Ausnahme der Vorschriften über den betrieblichen Datenschutzbeauftragten, über die Befugnisse und Pflichten der landesrechtlichen Aufsichtsbehörden und über die Meldepflichten. Diese Funktionen übernimmt auf der Ebene des Bundes der Bundesbeauftragte für den Datenschutz als externe Kontrollbehörde, wie sich aus § 19 Abs. 1 iVm § 7 Abs. 1 BDSG ergibt.

Für den Bereich der Länder konnte der Bundesgesetzgeber mangels Gesetzgebungskompetenz

keine entsprechende Regelung treffen. Daraus ergibt sich die Notwendigkeit, diese Lücke durch eine landesgesetzliche Regelung auszufüllen. Dementsprechend erklärt **§ 2 Abs. 1 Satz 2 E** die Vorschriften zur Durchführung des Datenschutzes und zur Überwachung durch den Datenschutzbeauftragten für anwendbar. Unabhängig davon gehört es zu den Aufgaben der allgemeinen Behördenaufsicht und der vom Staat über die Körperschaften und sonstigen juristischen Personen des öffentlichen Rechts ausgeübten Aufsicht, die Einhaltung der gesetzlichen Vorschriften zum Datenschutz auch im Bereich wirtschaftlicher Betätigung zu überwachen.

Eine Übernahme der §§28, 29 BDSG (betrieblicher Datenschutzbeauftragter) halte ich nicht für geboten. Diese Unternehmen unterliegen der Überwachung durch den Hessischen Datenschutzbeauftragten und sind an die Datensicherungsvorschrift nach § 15 Abs. 1 E gebunden. Danach haben sie dafür zu sorgen, daß die innerorganisatorischen Datenschutzmaßnahmen getroffen werden.

Im übrigen lassen die Verweisungen in § 22 Abs. 1 und § 31 Abs. 1 BDSG auf § 7 Abs. 2 Satz 1 Nr. 1 BDSG die Frage offen, ob zu den Voraussetzungen des § 7 Abs. 2 Satz 1 Nr. 1 auch der — im selben Satz 1 enthaltene — Vorbehalt gehört, daß der Datenschutz nicht durch Landesgesetz geregelt ist, oder ob sich die Verweisung nur auf den bloßen Wortinhalt der Nr. 1 bezieht, das hieße, auf die Aufsicht des Landes und auf die Ausführung von Bundesrecht. Dies kann hier jedoch dahingestellt bleiben (vgl. Rdnr. 2.10.1).

2.4.2 Nach § 1 Abs. 3 BDSG gilt der Datenschutz — mit Ausnahme des § 6 Abs. 1 — nicht für die Massenmedien, soweit sie personenbezogene Daten zu eigenen publizistischen Zwecken verarbeiten. Dies entspricht dem Grundrecht der Presse-, Rundfunk- und Filmfreiheit nach Art. 5 GG. Für das Landesrecht kommt eine entsprechende Regelung nur für die Anstalt des öffentlichen Rechts „Hessischer Rundfunk" in Betracht. Sie hat ihren Platz in **§ 2 Abs. 3 E.**

Der Ausschuß der Staatsaufsicht in § 1 Abs. 1 Satz 2 des Gesetzes über den Hessischen Rundfunk vom 2. 10. 1948 garantiert die Rundfunkfreiheit, die in der Verfassung des Landes Hessen nicht ausdrücklich genannt ist, im Sinne des später in Kraft getretenen Art. 5 GG. Davon bleibt jedoch die allgemeine Rechtsaufsicht der Landesregierung darüber, daß das Gesetz vom 2. 10. 1948 und die allgemeinen Gesetze beachtet werden, unberührt, — wie auch ein Vergleich mit der Rechtsstellung des dem Landesrecht zugeordneten „Zweiten Deutschen Fernsehens" (§ 25 des Staatsvertrages vom 6. 6. 1961) ergibt.

2.5 Die **Verantwortung** für die Verwaltungsaufgabe und die Haftung für Fehler bei ihrer Durchführung muß bei der für die Verwaltungsaufgabe zuständigen Behörden oder öffentlichen Stelle auch dann verbleiben, wenn die Daten von einer anderen Person oder Stelle im Auftragsverhältnis verarbeitet werden oder wenn die — automatisierte — Datenverarbeitung im ganzen aus der Verwaltung ausgelagert und behördlichen Rechenzentren übertragen wird.

2.5.1 Dieser Grundsatz ist in **§ 6 Abs. 1 E** festgelegt. § 14 E ergänzt diese Bestimmung. Die Bindung an die Weisungen des Auftraggebers ist die Voraussetzung für dessen Verantwortlichkeit.

Für den öffentlichen Bereich des Landes genügt diese Regelung; sie ersetzt die umständliche und wegen der vielen Verweisungen schwer verständlichen Regelung im § 8 BDSG.

2.5.2 Zugleich regelt **§ 6 Abs. 2 bis 4 E** die Haftung für Schäden, die den Betroffenen infolge einer unzulässigen Datenverarbeitung oder durch die Verarbeitung unrichtiger Daten entstehen. Die verantwortlichen Körperschaften sollen zur Wiedergutmachung des Schadens ohne weitere Voraussetzungen verpflichtet sein. Mit § 6 Abs. 2 des Entwurfs werden die Grenzen der — mittelbaren — Staatshaftung nach Art. 34 GG überschritten. Der Vorschlag beabsichtigt, eine unmittelbare Haftung des Staates oder der Körperschaften, die den Datenschutz im Sinne des § 6 Abs. 1 zu gewährleisten haben, einzuführen.

Art. 34 GG steht einer solchen Regelung nicht entgegen. Er garantiert die Staatshaftung nur in Mindestgrenzen, die nicht zum Nachteil des Bürgers unterschritten werden dürfen; er hindert den Gesetzgeber nicht, die Rechtsstellung des Bürgers gegenüber dem Staat und den öffentlich-rechtlichen Körperschaften zu verbessern und deren unmittelbare Staatshaftung zu begründen.

Die Ausweitung der Staatshaftung für die Datenverarbeitung ist geboten, weil den großen Vorteilen, welche die Datenverarbeitung der Verwaltung bietet, erhebliche Risiken für den Bürger gegenüberstehen. Erfahrungen der Vergangenheit — nicht nur in Hessen — haben hinreichend deutlich gemacht, welche Nachteile im einzelnen, besonders im Bereich der Leistungsverwaltung, entstehen können, wenn die verarbeiteten Daten unrichtig oder die Verarbeitungsprogramme fehlerhaft sind. Der einzelne ist außerstande zu beurteilen, ob die Benachteiligung, die er dadurch erleidet, ver-

schuldet ist und wer sie zu verantworten hat. Deswegen soll eine uneingeschränkte, vom Verschulden unabhängige und einer Exkulpation nicht zugängliche Haftung der für den Datenschutz verantwortlichen Behörden oder Stellen die materiellen Datenschutzrechte des einzelnen nach § 5 E ergänzen.

Gegen die Einführung einer solchen oder einer ähnlichen Ersatzpflicht in das BDSG ist zwar im Gesetzgebungsverfahren vom Rechtsausschuß und vom Finanzausschuß des Bundestages Widerspruch erhoben worden. Dies sollte jedoch den hessischen Gesetzgeber nicht abhalten, eine Wiedergutmachungs- und eine Schadensersatzpflicht des Staates bzw. der kommunalen Selbstverwaltungskörperschaften einzuführen. Eine nicht näher definierte Wiedergutmachungspflicht besteht im übrigen schon nach § 4 Abs. 2 HDSG.

In die Schadenersatzpflicht sollte – nach den von der Rechtssprechung entwickelten Grundsätzen über den Ausgleich immaterieller Schäden bei Persönlichkeitsrechtsverletzungen – auch der nicht vermögensrechtliche Schaden einbezogen werden.

2.6 Das wirksamste Mittel des Datenschutzes ist, das **Speichern, Verändern** und **Übermitteln** personenbezogener Daten nur unter engen Voraussetzungen zuzulassen und eine zeitlich unbegrenzte Verwendung der Daten durch die Verpflichtung zum **Sperren** und zum **Löschen** zu verhindern. Die Maßstäbe für solche Beschränkungen behördlicher Datenverarbeitung ergeben sich aus den Aufgaben der Behörde oder öffentlichen Stelle. So ist auch der zweite Abschnitt des BDSG aufgebaut. Jedoch ergibt sich aus § 3 BDSG, der als eine der „Allgemeinen Vorschriften" die drei Anwendungsbereiche des Bundesgesetzes umfaßt, daß auch die Einwilligung des Betroffenen eine selbständige Zulässigkeitsvoraussetzung ist, und zwar unabhängig davon, ob die spezifischen Voraussetzungen für die drei Anwendungsbereiche vorliegen.

2.6.1 Diese Regelung ist für den nicht-öffentlichen Bereich wohl unverzichtbar. Sie entspricht aber nicht dem für die öffentliche Verwaltung gültigen Grundsatz, daß jedes Verwaltungshandeln nur zur Erfüllung einer bestimmten Aufgabe im Rahmen der Bindung an Recht und Gesetz zulässig ist. Das bloße Einverständnis, das sich eine Behörde oder öffentliche Stelle von dem befragten Bürger erklären läßt, kann für sich allein die Verarbeitung personenbezogener Daten nicht rechtfertigen.

Jedoch müssen Ausnahmen von diesem Grundsatz für die Übermittlung personenbezogener Daten zugelassen werden. Die öffentliche Verwaltung soll befugt sein, Vorhaben im nicht-öffentlichen Bereich, die einem anerkannten allgemeinen Interesse der Bevölkerung dienen, durch Datenübermittlung zu unterstützen, sofern dadurch das Persönlichkeitsrecht der Betroffenen nicht verletzt wird. Die Voraussetzungen hierfür muß das Gesetz bestimmen. Sie sind in **§ 9 Abs. 2 E** festgelegt. Diese Regelung bietet einen höheren Datenschutz als der entsprechende § 11 Abs. 1 Satz 1 BDSG.

Eine allgemeine Bestimmung über die Zulässigkeit der Datenverarbeitung im Sinne des § 3 BDSG braucht daher in das Landesgesetz nicht aufgenommen zu werden. Der Vorrang besonderer Vorschriften zum Datenschutz in anderen Gesetzen wird in **§ 30 E** festgelegt; eine besondere Vorschrift im Sinne von § 3 Abs. 1 Nr. 2 BDSG ist daher ebenfalls entbehrlich.

2.6.2 Ob die Datenverarbeitung für die **Erfüllung der Aufgabe erforderlich** ist (§§ 7, 8, 9 E), muß nach strengen Maßstäben geprüft werden. Die Beurteilung muß ergeben, daß die Verwaltungsaufgabe ohne Verarbeitung personenbezogener Daten nicht sachgerecht und ordnungsmäßig erfüllt werden kann.

2.6.3 Eine **Einwilligung des Betroffenen** ist erforderlich, wenn er zur Auskunft rechtlich nicht verpflichtet, sondern es in sein Belieben gestellt ist, ob er sie gibt. Diese Entscheidungsfreiheit muß gesichert sein. Deswegen wird in **§ 7 Abs. 2 und 3 E** vorgeschlagen, für die Einwilligungserklärung die Schriftform, die genaue Beschreibung ihres sachlichen Inhalts und die Zusicherung des Ausschlusses von Rechtsnachteilen im Falle ihrer Verweigerung vorzuschreiben.

2.7 Die **Datenübermittlung an Stellen außerhalb** des öffentlichen Bereichs (§ 9 E), also an private Personen oder Unternehmungen darf nur ausnahmsweise gestattet sein. Personenbezogene Daten, die zur Erfüllung gesetzlicher Aufgaben gespeichert werden, dürfen dieser Zweckbestimmung grundsätzlich nicht entzogen und nicht für eine kommerzielle Verwertung im nicht-öffentlichen Bereich ohne Einwilligung des Betroffenen verwendet werden. Daher läßt **§ 9 Abs. 2 E** die Weitergabe nur zu, wenn außer dem Interesse, das der Empfänger nachweisen muß, auch die Einwilligung vorliegt. Nur unter besonderen Voraussetzungen kann auf den Nachweis der Einwilligung des Betroffenen verzichtet werden.

2.8 Der **Schutz der Vertraulichkeit** solcher personenbezogener Daten, die einem Berufs- oder besonde-

ren Amtsgeheimnis unterliegen, wird – gegenüber der Regelung in §§ 10 und 11 BDSG – in **§§ 8, 9 E** verschärft. Die Weitergabe dieser Daten an einen dritten Empfänger soll nur mit der Einwilligung des Betroffenen zulässig sein. Demgegenüber läßt es § 10 Abs. 2 Satz 2 BDSG – und in entsprechender Weise auch § 11 Satz 2 BDSG – genügen, daß der Dritt-Empfänger „die Daten zur Erfüllung des gleichen Zweckes" benötigt, bzw. sie unter den „gleichen Voraussetzungen" wie sein Vorbesitzer erhält. Diese Regelungen vernachlässigen das Schutzbedürfnis des Betroffenen zugunsten der Interessen der Verwaltung in unzumutbarer Weise, weil jeweils nur die empfangende Stelle – in eigener Sache – entscheidet, ob sie die Übermittlung fordern darf, und weil der Betroffene unbeteiligt bleibt, obwohl es sich um Daten handelt, an deren vertraulicher Behandlung wegen ihrer Art er schon bei der ersten Speicherung in erhöhtem Maße interessiert ist.

2.9 **§ 11 E** präzisiert und erweitert die Bestimmung des § 5 HDSG. Bei **Informationssystemen** und Erhebungen **für statistische, planerische oder ähnliche Zecke** soll dem Betroffenen der gleiche Schutz gegen eine zweckfremde Verwendung seiner Daten garantiert werden, wie er im Geltungsbereich des Statistikgeheimnisses seit langem besteht.

Informationssysteme dieser Art sind dadurch ausgezeichnet, daß sie zwar die Speicherung und interne Verarbeitung großer Mengen von personenbezogenen Daten voraussetzen, daß die von ihnen zu erstellenden Entscheidungshilfen, wie z. B. Statistiken, Tabellen, Indikatoren und thematische Karten, aber keine personenbezogenen Daten zu enthalten brauchen. Dem entspricht die in Absatz 1 und 2 getroffene Regelung: Personenbezogene Daten können an die Stelle, die ein Planungsinformationssystem betreibt, übermittelt werden; diese muß aber die spezielle Zwecksetzung strikt beachten. Insbesondere dürfen den Benutzern des Systems ausschließlich solche Daten zugänglich gemacht werden, die keine Rückschlüsse auf Einzelpersonen zulassen. Absatz 3 erstreckt diese Grundsätze auf Planungsumfragen und ähnliche Erhebungen.

2.10.1 Für die Datenverarbeitung der öffentlich-rechtlichen **Unternehmen** soll, soweit sie **am Wettbewerb** teilnehmen, grundsätzlich die Regelung für die entsprechenden Unternehmen auf Bundesebene gelten, nämlich die Vorschriften in § 22 Abs. 1 Satz 2 und § 31 Abs. 1 BDSG. Deswegen wird die Geltung des Gesetzes in § 2 Abs. 1 Satz 2 E auf Vorschriften beschränkt, auf die wegen der Zugehörigkeit dieser Unternehmen zur öffentlichen Verwaltung des Landes nicht verzichtet werden kann, vor allem die Überwachung durch den Datenschutzbeauftragten und die Mitteilungen für das Dateienregister.

Wie unter Rdnr. 2.4.2 dargelegt, bleibt es allerdings zweifelhaft, inwieweit die Regelung des BDSG in § 22 Abs. 1 und § 31 Abs. 1 die landesrechtlichen Wettbewerbsunternehmen erfaßt. Daher wird in **§ 16 E** vorgeschlagen, die dort aufgeführten Vorschriften des BDSG, welche die einzelnen Phasen des Datenschutzes und das Verfahren für die Auskunft, die Berichtigung, die Sperrung und die Löschung regeln, in das Landesgesetz ohne Rücksicht darauf einzubeziehen, ob Bundesrecht oder Landesrecht ausgeführt wird.

2.10.2 Die Vorschriften des Entwurfs gelten ebenso wie das HDSG auch für die **Datenverarbeitung im Rahmen wissenschaftlicher Aufgaben.** Den hier bestehenden tatsächlichen und rechtlichen Besonderheiten im Vergleich zur Verwaltung trägt **§ 17 E** Rechnung. Er stellt klar, daß der wissenschaftliche Zweck nicht von der Beachtung des Datenschutzes entbindet. Abs. 3 beschränkt die Nutzung strikt auf die wissenschaftliche Auswertung.

2.11 Im **dritten Abschnitt E** werden die §§ 6 und 12 HDSG mit folgenden Abänderungen des geltenden Gesetzestextes zusammengefaßt:

2.11.1 In **§ 17 Abs. 1 und Abs. 2 E** werden den dort genannten Behörden und öffentlichen Stellen der Landes- und der Kommunalebene übereinstimmend die Verpflichtung auferlegt, Auskünfte zu geben. Die – unbegründete – Unterscheidung zwischen Auskunfspflicht nach § 6 Abs. 1 und Auskunftsrecht nach § 6 Abs. 2 HDSG wird vermieden.

2.11.2 Abweichung von § 6 Abs. 2 HDSG wird auf eine Auskunftsverpflichtung gegenüber den in § 2 Abs. 1 Nr. 3 E genannten juristischen Personen des öffentlichen Rechts verzichtet. Aufgaben und Zuständigkeiten sind auf Organe der öffentlich-rechtlichen Körperschaften, Anstalten und Stiftungen in der Regel nach anderen Maßstäben als für die Organe der kommunalen Gebietskörperschaften verteilt, so daß das Problem des „Informationsgleichgewichts" nicht oder nicht in vergleichbarer Weise auftritt.

2.11.3 § 5 Abs. 3 HDSG entfällt, weil der Entwurf ebenso wie das BDSG nur personenbezogene Daten in den Datenschutz einbezieht. Daten und Daten-

bestände im Sinne des § 5 Abs. 3 HDSG werden von der Definition der personenbezogenen Daten in § 3 Abs. 1 E, der mit § 2 Abs. 1 BDSG übereinstimmt, nicht erfaßt, weil sie sich auf keine bestimmten oder bestimmbaren Personen beziehen.

2.11.4 In **§ 18 Abs. 3 E** wird das „öffentliche Interesse", das nach § 5 Abs. 3 letzter Satz HDSG der Auskunftsverpflichtung gegenüber dem Landtag nur ausnahmsweise entgegenstehen kann, konkret umschrieben.

2.12 Der **vierte Abschnitt E** regelt die Institution des **Hessischen Datenschutzbeauftragten.** Sie ist eine besondere, von der Rechtsstellung des Bundesbeauftragten für den Datenschutz nach § 17 ff. BDSG und von entsprechenden Einrichtungen anderer Länder des In- und Auslandes grundsätzlich abweichende Einrichtung des Hessischen Landesrechts. Der Hessische Datenschutzbeauftragte ist als eine beratende Institution zwischen Parlament und Regierung angesiedelt. Er ist keine Verwaltungsbehörde herkömmlicher Art; er hat weder Anweisungsbefugnisse noch Eingriffs- oder Anordnungsrechte. Seine Stellung innerhalb des organisatorischen Aufbaues des Landes ist in der Anlage II zum Vierten Tätigkeitsbericht[3]) charakterisiert.

Im Gegensatz hierzu ist der Bundesbeauftragte für den Datenschutz in die Exekutive integriert: Er wird vom Bundespräsidenten auf Vorschlag der Bundesregierung ernannt; er untersteht der Rechtsaufsicht der Bundesregierung und der Dienstaufsicht des Bundesministers des Innern. Im Falle seiner vorübergehenden Verhinderung bestellt der Bundesminister des Innern einen Vertreter, ohne dazu den Bundesbeauftragten hören zu müssen. Das Amt des Bundesbeauftragten ist ein Hauptamt; es kann nicht, wie in Hessen, nebenamtlich ausgeübt werden.

Die im HDSG gewählte Lösung verdient den Vorzug; sie gewährleistet eine größere Unabhängigkeit. Der Grundsatz einer möglichst weitgehenden Bundeseinheitlichkeit greift hier nicht durch.

Für die Regelungen in §§ 7 bis 15 HDSG, die ohne besondere Änderung ihres materiellen Gehaltes übernommen werden, wird jedoch eine andere, systematisch bevorzugte Gliederung vorgeschlagen; deren Verständnis erschließt sich im allgemeinen aus dem Text der Vorschriften.

2.12.1 **§ 24 E** erweitert das Auskunftsrecht nach § 13 HDSG. Um prüfen zu können, ob die Datenschutzvorschriften eingehalten werden, muß der Datenschutzbeauftragte die Programme, die den Ablauf der Datenverarbeitung, insbesondere der automatischen, bestimmen, kennen. Die Behörden und öffentlichen Stellen des Landes haben zwar schon bisher dem Datenschutzbeauftragten auf sein Verlangen die verfügbaren Programme bereitwillig vorgelegt. Anläßlich der Erarbeitung eines neuen Landesgesetzes über den Datenschutz ist es jedoch geboten, dieses Einsichtsrecht, das zwar aus dem Auskunftsrecht nach § 13 HDSG abgeleitet werden kann, ausdrücklich festzulegen. Das gleiche gilt für die weitere Verpflichtung der Behörden und öffentlichen Stellen des Landes, dem Datenschutzbeauftragten den Zutritt zu den Diensträumen zu gewähren, damit er die Datensicherungsmaßnahmen (vgl. die aus dem BDSG entnommene Anlage zu § 16 E) überprüfen kann.

2.12.2 **§ 26 E** soll dazu beitragen, daß in der Bundesrepublik die materiellen Datenschutzvorschriften in allen Anwendungsbereichen möglichst übereinstimmend gestaltet und verwirklicht werden. § 19 Abs. 5 BDSG bestimmt für den Bundesbeauftragten das gleiche.

2.13.1 Die übrigen Abweichungen vom Text des BDSG sind unwesentlich. Sie sind aus der als Anlage beigefügten Gegenüberstellung erkennbar und aus dem Text-Zusammenhang heraus verständlich. Daher habe ich davon abgesehen, sie im einzelnen zu erläutern.

2.13.2 Um den Leitgedanken zu verwirklichen, das Landesgesetz soweit wie möglich dem BDSG anzugleichen, ist auch dessen Terminologie übernommen worden. Andererseits sind einzelne Formulierungen des BDSG abgewandelt worden, damit die Lesbarkeit der Vorschrift verbessert und das Verständnis für die Ziele des Gesetzes erleichtert werden.

[3]) 8. HLT Drucks. 8/438, insbesondere in Abs. 2.6

3. TENDENZEN IM DATENSCHUTZRECHT

3 Tendenzen im Datenschutzrecht

3.1 In der Bundesrepublik

Mit der Verabschiedung des Bundesdatenschutzgesetzes ist seit dem Erlaß des hessischen Datenschutzgesetzes im Jahre 1970 die für die weitere Entwicklung des Datenschutzes in der Bundesrepublik bei weitem bedeutsamste Entscheidung gefallen.

Um einen umfassenden und einheitlichen Datenschutz sicherzustellen, sollten alle Länder bis zum Ende des Jahres Datenschutzgesetze erlassen. Erste Kontakte mit dem Ziel einer gewissen Koordinierung haben stattgefunden. Dies gibt dem Land die Möglichkeit, die Entwicklung des Datenschutzes auch weiterhin zu fördern.

Datenschutzprobleme von besonderem Gewicht werden durch die nach wie vor aktuelle Reform des Melderechts und die in diesem Zusammenhang vorgesehene Einführung eines Personenkennzeichens ausgeworfen. Der in der Anlage vorgelegte Entwurf eines Landesdatenschutzgesetzes könnte dazu beitragen, die insoweit bestehenden verfassungsrechtlichen Bedenken auszuräumen.

Der Regierungsentwurf eines Bundesmeldegesetzes, der die Vergabe eines bundeseinheitlichen Personenkennzeichens vorsah, ist in der abgelaufenen 7. Legislaturperiode des Bundestages nicht verabschiedet worden. Der Rechtsausschuß des Bundestages hat am 5. Mai 1976 den Entwurf eines Bundesdatenschutzgesetzes mit der Maßgabe gebilligt, „daß folgender Grundsatz beachtet wird: Die Entwicklung, Einführung und Verwendung von Numerierungssystemen, die eine einheitliche Numerierung der Bevölkerung im Geltungsbereich dieses Gesetzes ermöglichen (Personenkennzeichen) ist unzulässig".

Die Diskussion, ob, in welcher Form und mit welchem Verwendungsbereich ein Personenkennzeichen eingeführt werden soll, ist damit jedoch nicht beendet. Im Auftrage der Innenministerkonferenz wird gegenwärtig untersucht, welche Konsequenzen aus dem Scheitern des Bundesmeldegesetzes zu ziehen sind. Die EDV-technischen Vorbereitungen zur Vergabe und Verwaltung von Personenkennzeichen sind mit erheblichen Investitionen weitergeführt worden. Dies macht deutlich, daß die vom Rechtsausschuß des Bundestages angesprochene Problematik unvermindert aktuell ist. In einer auf Wunsch des Ministerpräsidenten abgegebenen Stellungnahme habe ich darauf hingewiesen, daß die „rechtliche Beurteilung sich an der spezifischen Funktion des Personenkennzeichens orientieren muß. Indem es eine bessere Identifizierung und Ordnung personenbezogener Informationen ermöglicht, erleichtert es zugleich die Konzentration und Zirkulation solcher Informationen. Aus der Perspektive des einzelnen ein keineswegs gleichgültiger Vorgang. Denn die Verbesserung des Informationsprozesses verschärft auch das Risiko eines Mißbrauchs personenbezogener Angaben. Die Frage nach der Verfassungsmäßigkeit des Personenkennzeichens ist insofern zu allererst eine Frage nach der Existenz eines ausreichenden und wirksamen Datenschutzes."

Nicht zuletzt auf die Erfüllung dieser verfassungsrechtlichen Anforderungen zielt der mit diesem Bericht präsentierte Gesetzesvorschlag. Er könnte für den Anwendungsbereich des Gesetzes eine tragfähige Basis für die Verwendung des Personenkennzeichens abgeben. Problematisch bleibt der übrige, insbesondere der nicht-öffentliche Bereich. Ob das Bundesdatenschutzgesetz den gestellten Anforderungen genügt, ist zumindest zweifelhaft. Von einem gleichwertigen und umfassenden Schutz des Bürgers vor einer unkontrollierten Verwendung seiner Daten kann im nicht-öffentlichen Sektor jedenfalls solange nicht gesprochen werden, wie es an einer effektiven — und das heißt auch präventiv wirkenden und über wirksame Eingriffsbefugnisse verfügenden — Datenschutzkontrolle fehlt.

3.2 Im Ausland

Die Entwicklung im Ausland war im Berichtszeitraum besonders interessant. Es wurden eine Reihe von Gesetzentwürfen und Resolutionen vorgelegt, in denen Überlegungen aus den Tätigkeitsberichten und aus meinen Kontakten mit ausländischen Sachverständigen und Politikern wiederzufinden sind. Zahlreiche Gespräche in Österreich, Schweden, Großbritannien, Frankreich, den USA und mit Vertretern des Europarates, der Europäischen Gemeinschaft und der OECD waren auch für meine Arbeit von Nutzen.

3.2.1 Frankreich

Der Justizminister hat im Herbst 1976 der Nationalversammlung den Entwurf eines Gesetzes zum Schutz der Freiheitsrechte des Bürgers bei der Datenverarbeitung vorgelegt („Projet de loi relatif

à l'informatique et aux libertés")[1]). Dieser Gesetzentwurf beruht auf der wissenschaftlichen Untersuchung einer Regierungskommission, die auch die Datenschutzüberlegungen in den europäischen Nachbarländern sowie bei den internationalen Organisationen berücksichtigt. Auch zwischen der Kommission und mir kam es zu einem ausführlichen Meinungsaustausch.

Der Entwurf ist noch nicht in der Nationalversammlung behandelt worden, und es ist gegenwärtig nicht abzusehen, wann dies der Fall sein wird. Wie das BDSG knüpft er die Schutzregelung an den Begriff der „personenbezogenen Informationen" (Daten), wobei er allerdings in Art. 1 den Schutzzweck in der Art einer Präambel – sehr viel weitergehend als das BDSG – präzisiert: „Die Datenverarbeitung muß sich unter Achtung des Privatlebens sowie der individuellen und kollektiven Freiheitsrechte entwickeln"[2]). Diese Generalklausel macht es – weitaus stärker als das BDSG – deutlich, daß auch bei der Datenverarbeitung die Rationalisierung dem Schutz der Freiheitsrechte untergeordnet bleiben muß.

Besonders interessant sind im französischen Gesetzentwurf die vorgesehene Kontrollinstanz, die Regelung der Datenverarbeitung und der Schutz der Rechte der Bürger.

Die Kontrollinstanz

Das dem hessischen Konzept des Datenschutzes zugrunde liegende Prinzip der sog. externen Kontrolle der Datenverarbeitung durch eine besondere Institution hat sich auch hier durchgesetzt. Der Entwurf sieht dafür eine weitgehend unabhängige „Commission Nationale Informatique et Libertés" vor, die aus Mitgliedern des Staatsrats (Conseil d'Etat), des Kassationshofs und weiteren qualifizierten Persönlichkeiten sowie einem Beauftragten der Regierung besteht. Die 12 Mitglieder der Kommission werden auf Vorschlag des Justizministers von der Regierung auf die Dauer von vier Jahren ernannt.

Die Kommission hat die Aufgabe

- „der Information, indem sie die Öffentlichkeit der Datenverarbeitung gewährleistet und auf Berichtsersuchen antwortet;
- der Kontrolle der Datenverarbeitung mit der Möglichkeit, die Gerichte einzuschalten;
- der Zusammenarbeit sowohl mit dem öffentlichen wie dem privaten Sektor zum Zwecke präventiver anstatt repressiver Arbeitsweise;
- Untersuchungen für die Regierung oder für die Gerichte vorzunehmen" (Begründung zum Entwurf, S. 3).

Insbesondere soll die Kommission „alle betroffenen Personen über ihre Rechte und Pflichten informieren, sich mit ihnen ins Benehmen setzen und die Einrichtungen zur Verarbeitung personenbezogener Informationen kontrollieren" (Art. 4 des Entwurfes).

Zur Stärkung der regionalen Einwirkungsmöglichkeiten der Kommission können regionale Unterkommissionen gebildet werden, denen sie Teile ihrer Aufgaben übertragen kann.

Die Regelung der Datenverarbeitung

Wegen der unterschiedlichen Gefährdung werden verschiedene Regelungen für Datenverarbeitung im öffentlichen und im privaten Sektor vorgesehen. Im öffentlichen Sektor soll eine obere Behörde nach Anhörung der Kommission darüber entscheiden, welche Aufgaben durch Datenverarbeitung zu erledigen sind. Die Entscheidung der Kommission kann durch den Staatsrat aufgehoben oder abgeändert werden. Für den Privatsektor wird lediglich verlangt, daß der Kommission jede geplante Datenverarbeitung angezeigt wird. Eine Bestätigung der Anzeige bedeutet die Erlaubnis zum Beginn der Datenverarbeitung.

Außerdem wird eine öffentlich einsehbare Liste geführt; sie enthält alle der Kommission zur Kontrolle vorgelegten Projekte. Jährlich legt die Kommission dem Präsidenten der Republik einen Tätigkeitsbericht vor, der veröffentlicht wird. Das Gesetz enthält auch detaillierte Regelungen für die transnationale Datenverarbeitung.

Die Rechte der Bürger

Unmittelbar zum Schutz der individuellen Freiheitsrechte dienen die Vorschriften in den Art. 23 bis 31 des Entwurfs, die sich mit der Befragung von Personen, der Zulässigkeit der Speicherung und den Abwehrrechten des Betroffenen befassen. Als Generalklauseln für diese Rechte bestimmen die Art. 2 und 3:

Art. 2 „Aucune décision juridictionelle ou administrative impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations.

Art. 3 Toute personne a le droit de connaître et de contester les informations et les raisonnements

[1]) Vorlage Nr. 2.516 der ersten Sitzung der Nationalversammlung in der 5. Legislaturperiode 1976/77.

[2]) „L'informatique doit se développer dans le respect de la vie privée, des libertés individuelles et des libertés publiques".

utilisés dans les traitements automatisés dont les résultats lui sont opposés“[3]).

Werden personenbezogene Daten von Personen erhoben, so müssen diese über die Freiwilligkeit oder über ihre Verpflichtung zur Angabe, über die Auswirkungen einer Verweigerung der Angabe und über die natürlichen oder juristischen Personen, an die die Daten weitergegeben werden, informiert werden (Art. 23). Die Speicherung von Informationen in personenbezogener Form ist grundsätzlich nur zulässig bis zur Zweckerreichung, oder wenn das Gesetz oder die Kommission etwas anderes bestimmt hat (Art. 24). Für bestimmte Datenarten gilt ein absolutes Speicherungsverbot, das nur mit ausdrücklicher Zustimmung des Betroffenen durchbrochen werden kann: Hiervon sind alle personenbezogenen Informationen umfaßt, die „direkt oder indirekt die rassische Herkunft oder die politische, philosophische oder religiöse Überzeugung oder die Gewerkschaftsangehörigkeit von Personen erkennen läßt“ (Art. 26 Abs. 1). Die Kirchen sowie religiöse, philosophische, politische oder gewerkschaftliche Gruppen dürfen jedoch automatisierte Mitglieder-Register unterhalten.

Ebenso wie im Bundesdatenschutzgesetz hat auch nach dem französischen Entwurf der Betroffene grundsätzlich ein Recht auf Auskunft, Berichtigung und Löschung, wobei gewisse Einschränkungen bezüglich der Staatssicherheit und medizinischer Daten vorgesehen sind:

Jeder, der seine Identität nachweist, kann bei den im öffentlichen Datenbankregister enthaltenen Stellen Auskunft über ihn betreffende Verarbeitung personenbezogener Daten verlangen (Art. 27). Sie muß den Inhalt der gespeicherten Daten wiedergeben und in klarer Sprache abgefaßt sein. Eine schriftliche Auskunft kann der Betroffene gegen Gebühr erhalten. Die Kommission kann für die betreffenden Datenverarbeitungsstellen Fristen für die Auskunftserteilung festlegen. Gegen eine Verweigerung der Auskunft oder bei Zweifeln über ihre Richtigkeit kann sich der Betroffene an die Kommission wenden, die sich zur Zulässigkeit der Verweigerung oder des Auskunftsverlangens äußert. Er kann verlangen, daß ihn betreffende unrichtige, unvollständige oder unklare Informationen oder solche, deren Speicherung verboten ist, berichtigt, vervollständigt, klargestellt oder gelöscht werden. Auf Verlangen des Betroffenen muß ihm die zuständige Stelle kostenlos eine Kopie der geänderten Speicherung übermitteln. Bei bestrittenen Informationen obliegt die Beweislast für deren Richtigkeit der speichernden Stelle, es sei denn, daß die bestrittenen Informationen von dem Betroffenen selbst freiwillig mitgeteilt worden sind (Art. 29).

Soweit sich das Berichtigungsrecht des Betroffenen auf Informationen bezieht, die die Staatssicherheit oder die Verteidigung betreffen, ist ein besonderes Verfahren vorgesehen, das von der Kommission veranlaßt wird (Art. 30).

Auskunft über medizinische Daten wird dem Betroffenen nur über einen von ihm bestimmten Arzt seiner Wahl erteilt (Art. 31).

Die Strafvorschriften des Entwurfs sehen Haftstrafen von zwei Monaten bis zu fünf Jahren und Geldstrafen von 2 000 bis 2 Mio Ffrs vor.

Übergangsvorschriften in den Art. 36 und 37 des Entwurfs sollen gewährleisten, daß die Datenschutzkontrolle nach und nach aufgebaut wird. So soll sich beispielsweise die Kommission zunächst mit dem Datenschutz in der öffentlichen Verwaltung und erst später mit dem Datenschutz im privaten Sektor befassen.

3.2.2 Großbritannien

Auf Einladung des britischen Data Protection Committee[4]) nahm ich in beratender Funktion an einem ausführlichen Gespräch dieses Gremiums in London teil. Die Gesprächsrunde unter Beteiligung sämtlicher Mitglieder des Data Protection Committee behandelte in ihrer fast siebenstündigen Sitzung die Datenschutz-Erfahrungen in Hessen vor dem Hintergrund der in Großbritannien bestehenden Datenschutz-Probleme.

Auch in Großbritannien scheint sich die Ansicht durchzusetzen, daß eine institutionelle Verankerung des Datenschutzes den Vorzug verdient. Die ursprünglich nicht zuletzt von Mitgliedern der Kommission vertretene Auffassung, eine vor allem mit Hilfe standesrechtlicher Grundsätze zu realisierende Selbstkontrolle reiche völlig aus, ist wohl mittlerweile fallengelassen worden. Für die Kommission ist insofern das hessische Modell gegenwärtig von zentraler Bedeutung. Anscheinend strebt sie eine Lösung an, die eine Kombination der schwedischen und der hessischen Regelung sein dürfte.

Schwierigkeiten bestehen bei der Frage, welche Befugnisse ein Datenschutzbeauftragter haben

[3]) Art. 2: „Keine Gerichts- oder Verwaltungsentscheidung, die die Wertung eines menschlichen Verhaltens einschließt, kann allein auf automatische Datenverarbeitung gegründet werden.

Art. 3: Jedermann hat das Recht, Informationen und Begründungen, die in der automatischen Datenverarbeitung verwendet werden, zu erfahren und zu bestreiten, wenn deren Ergebnisse ihm entgegengehalten werden.“

[4]) Vgl. V, 3.2.

sollte. Einerseits geht es darum, eine übermäßige Zentralisierung und die damit verbundene Bürokratisierung zu verhindern, andererseits meint man hier wohl, daß der Datenschutz Eingriffskomptenzen nahelegt. Wie in der Bundesrepublik zögert man aber, sich dafür auszusprechen, und zwar im Hinblick auf die überkommende Struktur von Regierung und Verwaltung. Offensichtlich ist gegenwärtig das Kostenproblem das entscheidende Argument, um eine Datenschutzgesetzgebung hinauszuschieben, wenn nicht sogar in Frage zu stellen. Man meint, die privaten Unternehmen könnten mit Rücksicht auf ihre ohnehin angespannte wirtschaftliche Lage keine zusätzliche Belastung mehr vertragen.

Einigkeit besteht über die Notwendigkeit, in einem zukünftigen Gesetz neben der institutionellen Kontrolle das Recht des Bürgers zu verankern. Dazu zählt nach Ansicht der Kommission in erster Linie das Auskunftsrecht, das allerdings nur auf der Grundlage eines Registers gehandhabt werden kann. Skepsis besteht jedoch im Hinblick auf die Wahrnehmung solcher Rechte durch die Bürger. Die Kommission geht wohl davon aus, daß die Betroffenen kaum davon Gebrauch machen werden, es sei denn, konkrete persönliche Konflikte hätten ihnen die Notwendigkeit des Datenschutzes bewußt gemacht.

Was den Anwendungsbereich einer gesetzlichen Regelung angeht, so ist man sich im Prinzip zwar einig, daß sie sowohl die staatliche Administration als auch die Privatwirtschaft erfassen muß. Im Gegensatz zu Frankreich geht man aber davon aus, daß die schärferen Maßnahmen für den privaten Bereich vorgesehen werden müssen. Eine starke Zurückhaltung besteht gegenüber jeder Annahme, die Interessen des Bürgers könnten in mindestens ebenso gravierender Weise durch Datensammlungen der staatlichen Administration gefährdet werden. Fragenkomplexe wie Austausch von Daten im Rahmen der öffentlichen Verwaltung und Konkretisierung der Amtshilfe haben bislang eine sehr untergeordnete Rolle gespielt.

Die Unterhaltung war für beide Beteiligten von Nutzen. Es hat sich erneut gezeigt, welche Ausstrahlung die hessische Regelung besitzt und welchen Wert ausländische Gremien darauf legen, die in Hessen gewonnenen Erfahrungen zu verwerten.

3.2.3 Niederlande

Die von der niederländischen Regierung eingesetzte Expertenkommission zur Vorbereitung eines Datenschutzgesetzes hat am 30. November 1976 einen Gesetzentwurf über „Personendaten-Systeme" vorgelegt[5]). An Ausführlichkeit der Regelung übertrifft der Entwurf alle bisher bekannten Gesetze und Gesetzentwürfe: Er enthält in 10 Abschnitten insgesamt 104 sehr detaillierte Artikel.

Zentrale Begriffe des Gesetzentwurfs sind das „Datensystem" und die Genehmigungsbehörde („Registration Board"). Der Begriff des Datensystems wird wie folgt definiert: „Datensystem bedeutet: Sammlungen personenbezogener Daten, auf die automatisch zugegriffen werden kann, oder die in einer Weise angeordnet sind, die es ermöglicht, sensitive Daten (Angaben über religiöse, philosophische oder politische Überzeugungen, Rassenzugehörigkeit oder Hautfarbe, Straf- oder Disziplinarregister wie auch medizinische oder psychologische Personendaten) daraus zu entnehmen und die in einer Weise benutzt werden können, daß personenbezogene Daten an Dritte gelangen" (Art. 1).

Die Funktion der Genehmigungsbehörde (Art. 4 ff.) läßt gewisse Parallelen zur schwedischen Dateninspektion erkennen, nämlich insoweit sie das Recht zur Eingriffskontrolle hat. Die aus einem Vorsitzenden und höchstens 10 Mitgliedern bestehende Behörde wird von der Königin (Regierung) ernannt. Die Behörde berät den Justizminister in Datenschutzfragen (Art. 8 Abs. 2); sie legt jährlich einen Tätigkeitsbericht vor (Art. 8 Abs. 3). Verordnungen zur Ausführung des Datenschutzgesetzes bedürfen der vorherigen Anhörung der Genehmigungsbehörde. Diese hat nicht nur ein Auskunfts- und Zugangsrecht (Art. 10) gegenüber allen Datenverarbeitern, sondern kann sogar die Durchsuchung von Wohnungen anordnen. Sie muß darüber innerhalb 24 Stunden dem Generalstaatsanwalt einen Bericht vorlegen (Art. 9). Die Genehmigungsbehörde führt über die aufgrund des Datenschutzgesetzes zu registrierenden Personendatensysteme ein öffentliches Register, das jedermann kostenlos zur Einsicht zugänglich ist (Art. 12).

Jede Verarbeitung personenbezogener Daten ist nach dem niederländischen Gesetzentwurf nur nach der Registrierung des betreffenden „Datensystems" in einem bei der Genehmigungsbehörde geführten öffentlichen Register erlaubt.

Die Registrierung kann unter bestimmten Voraussetzungen verweigert werden. Dann ist die Verarbeitung personenbezogener Daten verboten (Art. 21). Ähnlich wie bei der schwedischen Regelung ist also der Betrieb einer Datenbank nur aufgrund

[5]) Der Entwurf ist in englischer Übersetzung als Dokument Nr. EXP/Data Prot. (77) 2 am 24. Januar 1977 vom Europarat veröffentlicht worden.

eines Verwaltungsakts der Kontrollbehörde zulässig.

Für die Registrierung werden die Datensysteme in drei Kategorien eingeteilt: Datensysteme, die einer einfachen Erlaubnis bedürfen, Datensysteme, die einer qualifizierten Erlaubnis bedürfen und Datensysteme, die einer Konzession bedürfen. Unter die erste Kategorie (Art. 17) fallen z. B. Mitgliederdateien von Kirchen, Stiftungen und anderen Organisationen, Abonnentendateien von Zeitungen und Zeitschriften, Lohn- und Gehaltsdateien im Personalwesen, Finanz- und ähnliche Dateien, die sich auf Gläubiger und Schuldner beziehen, Kunden- oder Lieferanten- oder ähnliche Dateien sowie Kombinationen der genannten Dateien.

Zur zweiten Kategorie gehören alle Datensysteme, die nicht unter die erste oder dritte Kategorie fallen (Art. 18).

Zur dritten Kategorie gehören alle Datensysteme, aus denen personenbezogene Daten an Dritte weitergegeben werden, die auch sensitive Daten enthalten oder bei denen das Einsichts- und Berichtigungsrecht gemäß Art. 64 Abs. 1 d beschränkt werden soll (Art. 19).

Durch Kabinettsverordnung soll für die einzelnen Datensystem-Typen der ersten Kategorie festgelegt werden, welche personenbezogenen Daten in das System aufgenommen werden dürfen und auf welche Personen sich die Daten beziehen dürfen (Art. 34).

Zur Registrierung eines Datensystems durch einfache Erlaubnis bedarf es lediglich der Angabe, daß das System der ersten Kategorie gemäß Art. 17 Abs. 1 angehört sowie des Namens und der Adresse des Datenverarbeiters (Art. 22).

Die Registrierung von Datensystemen der zweiten Kategorie setzt zusätzlich voraus, daß der Datenverarbeiter eine Art „Satzung" vorlegt, nach deren Bestimmungen das Datensystem betrieben werden soll (Art. 23). Diese auch für die dritte Kategorie vorgeschriebene „Satzung" muß sich im Rahmen der Bestimmungen des Datenschutzgesetzes und der dazu ergangenen Rechtsvorschriften halten. Sie soll Mindestbestimmungen enthalten (Art. 37 Abs. 2) über:

a) Den Zweck, der mit der Einrichtung und der Benutzung des Datensystems verfolgt wird;
b) die Personenkategorien, über die Daten im Datensystem gespeichert werden;
c) das Höchstmaß von Daten, das über jede Person gespeichert werden darf;
d) die Personen oder Personenkategorien, die Zugriff auf das Datensystem haben sollen;
e) die Personen innerhalb und außerhalb der Institution des Datenverarbeiters und die Stellen sowie die Arten von Personen und Stellen, an die Daten aus dem System weitergegeben werden;
f) die Frage, welche personenbezogenen Daten an Personen und Stellen unter Ziffer e) weitergegeben werden dürfen;
g) die Fälle, in denen gespeicherte Daten gelöscht werden dürfen;
h) die Ausführung der Vorschriften in den Art. 67, 69, 75 oder 76 (Anmelde-, Auskunfts-, Protokollierungs- und Informationspflicht);
i) eine Beschreibung der Organisation des Datensystems, insbesondere in Bezug auf seine Leitung.

Zur Registrierung der einer Lizenzpflicht unterworfenen Datensysteme muß der Datenverarbeiter der Genehmigungsbehörde ein Exemplar der „Satzung", eine Beschreibung der technischen Vorkehrungen und organisatorischen Maßnahmen für die Sicherheit des Systems sowie alle weitere Information vorlegen, der die Genehmigungsbehörde zur Entscheidung über die Erteilung einer Konzession bedarf (Art. 40). Die Behörde veröffentlicht den Antrag auf Konzessionserteilung im Niederländischen Staatsanzeiger oder in einer Weise, die sie für angemessen hält, damit der Antrag den Personen, deren Daten in dem System gespeichert werden sollen, zur Kenntnis kommt (Art. 42). Die Konzession kann zeitlich begrenzt und mit Auflagen verbunden werden (Art. 45).

Grundsätzlich muß jeder Betroffene spätestens einen Monat nach der ersten Einspeicherung darüber unterrichtet werden, daß Daten über ihn in einem Datensystem gespeichert sind (Art. 63). Darüber hinaus ist jedermann auf dessen Antrag darüber Auskunft zu geben, ob und welche ihn betreffende personenbezogene Daten gespeichert und wohin sie weitergegeben worden sind. Sind Daten unrichtig, unvollständig, entgegen der Zweckbestimmung des Registers oder in Verletzung der „Satzung" gespeichert, so sind auf Antrag des Betroffenen die Daten zu berichtigen, zu ergänzen oder zu löschen. In gleicher Weise ist der Datenverarbeiter verpflichtet, gespeicherte Daten zu ergänzen, wenn sie unvollständig gespeichert sind (Art. 70).

Im übrigen enthält der Entwurf Bestimmungen über Schadensersatz (Art. 90), „internationale Aspekte" der Datenverarbeitung (Art. 91—93) sowie Strafbestimmungen (Art. 94—96).

3.2.4 Schweden

Im Rahmen der regelmäßigen Kontakte mit der schwedischen Dateninspektion[6]) fand im Novem-

[6]) Vgl. IV, 1.4; V, 3.2.

ber 1976 ein weiterer mehrtägiger Erfahrungsaustausch statt, diesmal in Stockholm. Schwerpunkte der Gespräche waren Datenschutzprobleme bei der Verwendung eines Personenkennzeichens und Erfahrungen auf dem Gebiet des Datenschutzes bei einem Krankenhausverbundsystem.

3.2.4.1 In Schweden wurde bereits kurz nach dem Zweiten Weltkrieg im Zusammenhang mit dem Volkszählungsregister durch die Einwohnermeldeverordnung von 1947 eine dreistellige „Geburtsnummer" eingeführt. Sie wurde Bestandteil der Personalnummer, die jede in Schweden gemeldete Person nach § 7 der Einwohnermeldeverordnung (Folkbokföringsförordningen von 1967/198) und § 4 des dazu ergangenen Erlasses (Folkbokföringskungörelsen von 1967/495) erhält, und die aus 10 Ziffern besteht. Die ersten sechs Ziffern enthalten das Geburtsdatum in der Reihenfolge Jahr, Monat, Tag und die nächsten drei Ziffern die Geburtsnummer; die letzte Ziffer ist eine Prüfziffer. Bei den Geburtsnummern werden ungerade Ziffern für Männer, gerade für Frauen verwendet. Aus der Personalnummer 380425-6653 beispielsweise ist erkennbar, daß es sich um eine männliche Person handelt, die am 25. April 1938 geboren ist. Die Personalnummer hat inzwischen die Funktion eines allgemeinen Identifikationszeichens erhalten und wird nicht nur im Einwohnermeldewesen benutzt, sondern auch beispielsweise als Wehrstammnummer, Sozialversicherungsnummer, als Halternummer für das Kraftfahrzeugregister, für den Führerschein, als Paßnummer und Nummer für Seeleute, für Zwekke des Erziehungswesens sowohl wie — mit Zusatzziffer — als Steuernummer.

Aufgrund des in Schweden traditionellen Prinzips der Aktenöffentlichkeit[7]) ergab sich beinahe zwangsläufig die Folge, daß sich auch die Privatwirtschaft des Personenkennzeichens bemächtigt hat. Sowohl Behörden gegenüber als auch im Schriftverkehr mit Firmen wird von dem schwedischen Bürger heute normalerweise die Angabe seines Personenkennzeichens verlangt. Durch das für fast alle Lebensbereiche verwendete Personenkennzeichen ist die Verknüpfbarkeit von Informationen über eine Person mit Hilfe der EDV entscheidend verstärkt worden. Die Gefahr, ein „transparenter Bürger" zu werden, hat sich erhöht.

3.2.4.2 Im Hinblick auf das in Hessen in Entwicklung befindliche Projekt eines Datenverarbeitungs-Verbundes für mehrere Krankenhäuser[8]) waren die Erfahrungen von besonderem Interesse, die in Schweden mit den dort bereits seit mehreren Jahren bestehenden computergestützten medizinischen Informationssystemen für den Bereich mehrerer Krankenhäuser gemacht worden sind. Für die Region Groß-Stockholm besteht ein medizinisches Informationssystem für etwa 20 Krankenhäuser mit den entsprechenden Daten der ca. 1,6 Mio Bewohner des Verwaltungsbezirks. Die Datenbank enthält für jeden erfaßten Bewohner dessen allgemeine Daten, Angaben über einzelne Behandlungen im Krankenhaus mit Stichworten seiner Krankengeschichte, Angaben über Röntgenuntersuchungen, Daten über Einlieferung und Entlassung und Vormerkungen für ambulante Behandlungen. Das System basiert auf einer zentralen Computereinrichtung mit über 200 on-line untereinander verbundenen Terminals. Die Anfänge des Systems gehen auf 1967 zurück; seine jetzige Ausbaustufe erreichte es 1971. Das Informationssystem ermöglicht es dem behandelnden Arzt, bei Einlieferung beispielsweise eines Unfallpatienten, sofort dessen Blutgruppe, Angaben über frühere stationäre Behandlung, Medikamenten-Empfindlichkeit sowie die wichtigsten Angaben zur Krankengeschichte auf Bildschirm abzurufen. Detailangaben der Krankengeschichte können nur von Arzt zu Arzt mündlich oder schriftlich weitergegeben werden. Dadurch soll die Gefahr vermieden werden, daß gespeicherte Daten ohne ihre sog. Kontextbezogenheit — d. h. den Gesamt-Zusammenhang, in dem sie erhoben wurden, wie Ort, Zeit, besondere Situation des Patienten — leicht ein unzutreffendes Bild für die Diagnose ergeben. Besonders sensitive Daten, wie z. B. psychiatrische Daten, dürfen überhaupt nicht per EDV übermittelt werden, sondern nur schriftlich von Arzt zu Arzt.

Den Kern der für das System eingerichteten Datenschutzmaßnahmen bildet eine abgestufte Zugriffsregelung, die durch einen genau festgelegten internen Sicherheits-Code, der sich von Zeit zu Zeit ändert, ergänzt wird. Es bestehen 4 Zugriffskategorien mit folgender Benutzerbeschreibung:

Kategorie 1:
Benutzer, die Patientendaten nur zu Verwaltungszwecken, insbesondere zur Abrechnung, benötigen.

Kategorie 2:
Benutzer, wie Krankenschwestern und Laborpersonal, die zwar medizinische Daten des Patienten brauchen, aber nicht die Kenntnis der Krankengeschichte oder Diagnose.

Kategorie 3:
Benutzer, wie Ärzte und Personal der Notfall-Abteilung, die auf sämtliche medizinische

[7]) Vgl. II, 2.3.5.

[8]) Dominig II, vgl. II, 4.1.1.3; V, 1.5.

Daten des Patienten Zugriff haben müssen.

Kategorie 4:
Bisher noch nicht festgelegt (evtl. Zugriff auf aggregierte Daten für Planung, Statistik und Forschung).

Auch Ärzte haben unmittelbaren Zugriff nur auf die Daten der Kategorie 3, die sie selbst eingespeichert haben; so kann ein Arzt z. B. nur Daten über die von ihm in seiner Abteilung behandelten Patienten abrufen. Benötigt er Daten aus anderen Abteilungen, so ist dies (siehe oben) wegen der Kontextbezogenheit nur über den dort behandelnden Arzt möglich.

Jeder Patient hat das Recht auf einen Ausdruck der über ihn gespeicherten Daten. Dieser Ausdruck muß von dem Arzt, der den Patienten zuletzt behandelt hat, unterzeichnet sein. Für den Fall, daß der Arzt Bedenken hat, die Information könne sich nachteilig auf den Gesundheitszustand des Patienten auswirken, kann er den betreffenden Teil des Ausdrucks dem Patienten vorenthalten. Dieser kann sich dagegen mit einer Beschwerde an den Verwaltungsrat des Krankenhauses wenden, und wenn dieser der Beschwerde nicht abhilft, an das Oberverwaltungsgericht. Bei 2 000 Auskunftsfällen gab es nur 2, in denen aus medizinischen Gründen die Auskunft partiell verweigert wurde. Von den ca. 1,6 Mio Einwohnern, deren Daten im System gespeichert sind, kommen etwa 1 bis 2 Auskunftsbegehren pro Woche; lediglich im ersten Monat nach Einführung des Auskunftsrechtes (Juli 1974) kamen ca. 1 500 Auskunftsbegehren.

Nach Auffassung der Beteiligten hat sich das Krankenhaus-Informationssystem bewährt.

3.2.5 USA

In den USA sind auf Bundesebene neue Gesetzgebungsinitiativen von der zweiten Jahreshälfte 1977 an zu erwarten, nachdem die Studienkommission für Datenschutz[9]) dem Präsidenten und dem Kongreß ihren Abschlußbericht vorgelegt hat mit Empfehlungen für gesetzgeberische oder administrative Maßnahmen, um „das Persönlichkeitsrecht des einzelnen unter Abwägung mit den berechtigten Informationsbedürfnissen der Regierung und der Gesellschaft zu schützen“[10]).

Jedoch enthalten bereits der im Juni 1976 vorgelegte Zwischenbericht der Kommission sowie der gemäß Art. 3 Abs. (p) des amerikanischen Datenschutzgesetzes[11]) zum 30. Juni eines jeden Jahres vom amerikanischen Präsidenten dem Kongreß vorzulegende Jahresbericht über die Entwicklung der Datenverarbeitung in der Bundesverwaltung interessante Hinweise zur Entwicklung des Datenschutzes in den USA. So ist dem Bericht des Präsidenten zu entnehmen, daß der Erlaß des Datenschutzgesetzes zu Einschränkungen der elektronischen Datenverarbeitung und bei der Verwendung eines Personenkennzeichens führte: Mehrere Behörden haben auf den Betrieb eigener Datenbanken verzichtet, andere deren Benutzung stark eingegrenzt: die bisher verbreitete Benutzung der Sozialversicherungsnummer als Personenkennziffer auch für andere Bereiche wurde eingeschränkt.

Aus dem Zwischenbericht der Kommission lassen sich drei Arbeitsschwerpunkte erkennen:

1. Die Auswertung der Untersuchungen über die gegenwärtige Praxis und Zielrichtung der elektronischen Datenverarbeitung in öffentlicher Verwaltung und Privatwirtschaft;
2. die Studie über bereichsübergreifende Datenschutzprinzipien, die sich hauptsächlich mit Grundsatzfragen zur Abgrenzung des Schutzes des Persönlichkeitsrechts von den gesellschaftlichen Notwendigkeiten der Informationsfreiheit befaßt;
3. die Stellungnahme zur künftigen Entwicklung der Datenverarbeitung, die sich mit den Trends der Computer-Technologie und ihren Auswirkungen auf den Schutz des Persönlichkeitsrechts befaßt.

Die Konkretisierung dieser Schwerpunkte ist im Juni 1976 Gegenstand eines eingehenden Gesprächs zwischen der Kommission und mir gewesen. Im Mittelpunkt stand dabei ein Fragenkomplex, dem auch für Hessen eine besondere Bedeutung zukommt: der Datenschutz im Gesundheitswesen. Der Meinungsaustausch mit der Kommission bezog sich aber auch auf die Kontrollmöglichkeiten bei Polizeiinformationssystemen. In den Vereinigten Staaten liegen bereits, wie sich am Beispiel Kalifornien zeigt, konkrete Regelungen vor, Sie werden durch den Versuch gekennzeichnet, sorgfältig zwischen den einzelnen Informationen zu unterscheiden und von der Grundlage dieser Unterscheidung dem Bürger auch im polizeilichen Bereich einen Anspruch auf Benachrichtigung, Berichtigung und Löschung zu garantieren.

Besondere Beachtung verdient der vom Domestic Council Committee on the Right of Privacy dem Präsidenten der Vereinigten Staaten vorgelegte

---

[9]) Art. 5 Abs. (g) des USA-Datenschutzgesetzes; vgl. deutsche Übersetzung in Heft 3 der „Beiträge zum Datenschutz“ des Hessischen Datenschutzbeauftragten, S. 42.

[10]) aaO. Abs. b (2), S. 35

[11]) vgl. aaO., S. 32

Bericht über die nationale Informationspolitik. Er geht auf ein Problem ein, das nicht zuletzt im Hinblick auf das Bundesdatenschutzgesetz auch für die Bundesrepublik unmittelbar praktische Bedeutung besitzt. Die Erfahrung in den Vereinigten Staaten hat gezeigt, daß allgemeine Formulierungen, wie sie sich in den meisten Datenschutzregelungen finden, am Verhalten der öffentlichen Verwaltung letztlich wenig ändern. Zwar wird jede dieser Formeln zur Kenntnis genommen ohne aber, was der Absicht des Gesetzgebers entsprochen hätte, in konkrete Maßnahmen umgesetzt zu werden. Die Kommission zieht daraus die Folgerung, daß der Gesetzgeber so schnell wie möglich bereichsspezifische Regelungen vorlegen muß. Nur so könne die einer Verwirklichung des Datenschutzes hinderliche Abstraktionsebene verlassen werden.

Vor dem Hintergrund dieser Entwicklung ist auch die Initiative der Abg. Koch und Goldwater zu sehen. Sie haben am 21. 9. 1976 dem Repräsentantenhaus einen Gesetzentwurf[12]) vorgelegt, der das Datenschutzgesetz von 1974 ergänzen, „einige Schlupflöcher schließen und Ausnahmen beenden (soll), die sonst eine dauernde und unerträgliche Durchleuchtung von Privatangelegenheiten unserer Bürger durch Staat, Kommunalverwaltungen und Privatpersonen ermöglichen würden"[13]). Der angestrebte „Right to Private Records Act" soll Datenschutzbestimmungen speziell für das Bank- und Kreditwesen — inklusive Sparkassen, Bausparkassen, Heimstättenverbände oder Kreditvereinigungen — sowie für das Fernmeldewesen bringen, insbesondere hinsichtlich des Informationsrechts staatlicher Stellen.

Nach dem Entwurf sollen künftig auf den genannten Gebieten personenbezogene Daten von staatlichen Stellen nur noch gefordert oder an diese weitergegeben werden dürfen, wenn der Betroffene schriftlich zugestimmt hat, oder wenn die Weitergabe aufgrund einer gesetzlich zulässigen Verwaltungs- oder Gerichtsanordnung oder eines Durchsuchungsbefehls erfolgt (§ 3 [a] [1]). Für Daten, die nicht auf eine bestimmte Person bezogen oder beziehbar sind, soll das Gesetz nicht gelten. Werden Daten entgegen den Vorschriften des geplanten Gesetzes weitergegeben, so soll der Betroffene ein Recht auf Ersatz des Schadens, mindestens in Höhe von 1000 Dollar haben, bzw. auf 100 Dollar, multipliziert mit der Anzahl der Tage, an denen die unberechtigte Datenweitergabe erfolgte (§ 11); außerdem sind Strafbestimmungen (§ 12) vorgesehen.

Zu dem Gesetzeszweck führte Abg. Koch weiter aus: „Nachdem der Bundesregierung diese häßlichen Praktiken versagt wurden (durch das Datenschutzgesetz von 1974) sollten auch Staatsregierungen und Kommunalverwaltungen sowie Personen und Organisationen auf dem privaten Sektor nicht mehr nach Laune oder ohne genügenden Grund uneingeschränkten Zugriff auf Kredit-, Bank- oder Versorgungsdaten eines Bürgers haben dürfen."[13]).

Der Entwurf soll außerdem Probleme im Zusammenhang mit Abhören von Telefongesprächen lösen.

In einem weiteren Bereich der Datenschutzgesetzgebung des Bundes zeichnet sich eine neue Entwicklung ab: Wie der Kommission im November 1976 berichtet wurde, hat das Ende 1974 in Kraft getretene „Gesetz über Elternrecht und Datenschutz"[14]) mehr Probleme geschaffen, als es gelöst hat[15]). Es wird ausgeführt, daß das Gesetz zwar den Einrichtungen auf dem Gebiete des Erziehungswesens die Notwendigkeit des Datenschutzes zum Bewußtsein gebracht habe; die Praxis des Gesetzes lasse jedoch in vieler Beziehung zu wünschen übrig, da sie uneinheitlich sei. Es ist also zu erwarten, daß auch auf dem Gebiet des Datenschutzes im Erziehungswesen neue gesetzgeberische Maßnahmen vorbereitet werden.

Zwei Einzelstaaten haben inzwischen eigene Datenschutzgesetze erlassen, nämlich Virginia am 8. April 1976 und Ohio am 21. Juli 1976.

Das Datenschutzgesetz von Virginia enthält vier Regelungsbereiche. Der erste enthält allgemeine Datenschutz-Grundsätze; der zweite regelt die Erfordernisse für Behörden; im dritten Abschnitt sind die Datenschutzrechte des Bürgers enthalten. Im letzten Abschnitt wird die Benutzung der Sozialversicherungsnummer auf die Fälle eingeschränkt, in denen dies durch Bundes- oder Landesgesetz vorgeschrieben ist; darüber hinaus wird der Rechtsweg für Datenschutzverletzungen geregelt.

Das Datenschutzgesetz von Ohio enthält zu dem vorgenannten einen wesentlichen Unterschied: § 1347.02 sieht die Schaffung eines mit weitreichenden Befugnissen ausgestatteten „Personal Information Control Board" (Datenschutz-Kontrollbehörde) vor. „Die Behörde soll die Vorschriften des Kapitels 1347 des Landesgesetzbuches in bezug auf Kommunalverwaltungen anwenden und durchsetzen. Die Behörde soll außerdem dem Parlament Empfehlungen unterbreiten für die Anwendung und Durchsetzung des Gesetzes bezüg-

[12]) House Report 15.657.

[13]) Abgeordneter Koch bei seiner Einbringungsrede; Congressional Record-House/H 10.747 vom 21. Sept. 1976.

[14]) „Buckley Amendment"; vgl. IV, 4.7.3.

[15]) The Washington Post vom 14. 11. 1976.

lich der durch Kommunalverwaltungen unterhaltenen Datenbanksysteme" (§ 1347.02 [C]). Das Gesetz regelt sehr ausführlich die Verpflichtungen von Behörden, die Datenverarbeitung betreiben, sowie die Rechte des betroffenen Bürgers (§ 1347.05–10).

3.2.6 Kanada

Am 24. 11. 1976 hat der kanadische Justizminister dem Parlament den Entwurf eines Gesetzes vorgelegt „Canadian Human Rights Act"[16]), das sich auf den Schutz der Menschenrechte bezieht, einschließlich des Rechts des einzelnen auf Zugang zu Informationen, die bei Regierungsstellen über ihn gespeichert sind. Das geplante Gesetz soll vor allem dazu dienen, jegliche Diskriminierung eines Bürgers zu verhindern, gleichviel, ob sie aus Gründen der Rasse, der Herkunft, der Hautfarbe, der Religion, des Alters, des Geschlechts, des Personenstands, der Körperbehinderung oder aufgrund einer Verurteilung geschieht. Zu diesem Zweck sieht es die Errichtung einer Menschenrechtskommission vor, deren – von der Regierung ernannte – Mitglieder unabhängig sind und nur aus den gleichen Gründen wie ein Richter von ihrem Amt abberufen werden können (§§ 21 ff.).

Der Datenschutz wird in Abschnitt IV „Schutz persönlicher Information" geregelt (§§ 49 bis 62). Ein Mitglied der genannten Menschenrechtskommission wird auf Vorschlag ihres Präsidenten vom Justizminister zum Datenschutzbeauftragten (Privacy Commissioner) ernannt (§ 57). Die Unabhängigkeit der Stellung des Datenschutzbeauftragten ist mit der des „Auditor-General" (Präsident des Rechnungshofes) vergleichbar. Wie dieser legt er dem Parlament mindestens einmal im Jahr einen Tätigkeitsbericht vor (§ 60), zu seiner Aufgabe gehört die Prüfung der Beschwerden von Bürgern, die meinen, daß man ihnen Rechte vorenthält, „in bezug auf sie betreffende personenbezogene Information, die in einer Datenbank der Bundesverwaltung gespeichert ist" (§ 58 Abs. 1). Für die Untersuchung solcher Beschwerden stehen dem Datenschutzbeauftragten die gleichen Befugnisse zu (§ 58 Abs. 5) wie dem „Human Rights Tribunal", das die Menschenrechtskommission zur Aufklärung von Verstößen gegen dieses Gesetz bilden kann, d. h. er hat richterliche Funktionen: Vernehmung und Vereidigung von Zeugen, Vorlage von Beweisen (§ 40 Abs. 3), Verbot gegenüber einer Person, eine bestimmte Tätigkeit fortzusetzen, Anordnungen gegenüber einer Person, einem anderen bestimmte Tätigkeiten in Ausübung seiner Menschenrechte zu gestatten und die Verurteilung zum Schadensersatz (Art. 41 Abs. 2 bis 4). Eine solche Entscheidung kann durch den „Federal Court of Appeal" (entspricht Bundesgerichtshof) überprüft werden.

Die unmittelbaren Datenschutzrechte des Bürgers regelt § 52: Danach hat jedermann das Recht auf Auskunft darüber, welche Daten über ihn in Datenbanken der – etwa 89 im Anhang des Gesetzes aufgeführten – Stellen der Bundesverwaltung gespeichert sind; er hat Anspruch auf Auskunft darüber, für welche Zwecke diese Daten seit Inkrafttreten des Gesetzes verwendet worden sind; er hat das Recht, die gespeicherten Daten oder einen Ausdruck davon zu überprüfen; er hat ein Berichtigungsrecht, wenn die gespeicherten Daten unrichtig oder unvollständig sind und für den Fall, daß eine Berichtigung verweigert wird, kann er verlangen, daß die Daten mit einer entsprechenden Anmerkung versehen werden. Wenn Daten, die vom Betroffenen durch Regierungsstellen für einen bestimmten Zweck erhoben worden sind, für einen anderen Zweck verwendet werden sollen, so darf dies nur mit seiner Zustimmung geschehen. Der Betroffene kann sich zur Durchsetzung seiner Rechte nach dem Datenschutzgesetz selbst oder durch einen Bevollmächtigten an den Datenschutzbeauftragten wenden.

Die genannten Auskunfts- oder Berichtigungsrechte können eingeschränkt werden, wenn ihre Ausübung schädlich für die internationalen Beziehungen, die nationale Sicherheit Kanadas oder die Beziehungen zwischen Bund und Provinzen sein könnten oder wenn dadurch die Verbrechensbekämpfung bzw. die öffentliche Sicherheit und Ordnung behindert würde (§ 53).

Der Gesetzentwurf enthält außerdem eine Reihe von Verwaltungsvorschriften, die verhindern sollen, daß Regierungsstellen in unnötigem Ausmaß von einzelnen bzw. Firmen Informationen sammeln. Dazu gehören insbesondere die Bestimmungen über Koordination von Datenbanken (§ 56), die dazu dienen sollen, den gegenwärtigen Informationsfluß zwischen den staatlichen Behörden festzustellen und zu koordinieren; ebenso die Vorschriften in § 62, die es der Regierung ermöglichen sollen, für bestimmte Kategorien von Daten (z. B. medizinische Daten) bereichsspezifische Regelungen zu treffen.

3.2.7 Australien

In Australien befassen sich zwei Gremien mit Fragen des Schutzes der Privatsphäre: Einmal die 1973 gebildete Regierungskommission für Rechtsreform (The Law Reform Commission), zum anderen das Privacy Committee von New

[16]) Bill C-25, Second Session, Thirtieth Parliament, 25 Elisabeth II, 1976, The House of Comons of Canada, 21882.

South Wales, einem der industriell am meisten entwickelten Staaten des australischen Bundesstaates.

Für die Law Reform Commission ist der Schutz der Privatsphäre nur eines aus einer Reihe von Problemen der Rechtsreform, an denen sie arbeitet[17]), während sich das Privacy Committee von New South Wales ausschließlich mit Problemen des Schutzes der Privatsphäre beschäftigt.

Die Commission hat beschlossen, sich zunächst auf folgende Kategorien der Untersuchung zu spezialisieren: Privatsphäre und Regierung, Privatsphäre und Medien, Privatsphäre und Verbraucher, Privatsphäre und privater Sektor. Sie unterstützt darüber hinaus die Arbeiten des Privacy Committee von New South Wales.

Das Privacy Committee von New South Wales ist eine ständige Einrichtung, die aufgrund eines Gesetzes von 1975 gebildet wurde. Es besteht aus 13 vom Gouverneur ernannten Mitgliedern. Nach den Vorschriften des Gesetzes gehören dem Gremium je ein Abgeordneter der Regierung und der Opposition, zwei Verwaltungsbeamte, zwei Mitglieder von Universitäten und vier Persönlichkeiten an, die besondere Erfahrungen oder besonderes Interesse auf dem Gebiete des Schutzes der Privatsphäre haben.

Auch der Ombudsman gehört dem Committee kraft Amtes an. Eines der Mitglieder ist hauptamtlich als geschäftsführendes Mitglied tätig; ihm steht ein kleiner Stab von Mitarbeitern für Forschung und Überprüfung von Beschwerden zur Verfügung.

Die Gründung dieser ständigen Einrichtung schien vor allem deshalb notwendig, damit ein Fachgremium entstand, welches die weit auseinanderlaufende Diskussion über den Schutz der Privatsphäre wissenschaftlich analysieren und zu konkreten Vorschlägen ausarbeiten konnte. Die Vorschläge reichten von der Schaffung eines neuen Haftungstatbestandes („Tort") über die Erarbeitung von Standesregeln für Datenverarbeiter und den Erlaß spezifischer Gesetze bis zur Schaffung eines unabhängigen Datenschutzausschusses.

Das Privacy Committee von New South Wales hat hauptsächlich die Aufgaben der Forschung und Entwicklung einer allgemeinen Richtlinie („policy") zum Schutz der Privatsphäre und der Untersuchung und Beratung von Einzelproblemen; es soll Beschwerden über unvertretbare Einschränkungen der Privatsphäre von jedermann entgegennehmen, untersuchen und dabei vermitteln; darüber hinaus wirkt es als Koordinierungsstelle für Informationen über den Schutz der Privatsphäre und regt die öffentliche Diskussion und die Forschung über Probleme des Schutzes der Privatsphäre an; schließlich soll das Committee Empfehlungen für neue gesetzliche Vorschriften und für Änderungen in Verwaltungs- und Geschäftspraktiken geben[18]). Zur Ausführung seiner Aufgaben hat das Committee das Recht, jedermann um Informationen zu bitten und zur Vorlage von Dokumenten zu ersuchen. Dies betrifft sowohl den öffentlichen als auch den privaten Bereich. Es hat aber keine Befugnis, seine Empfehlungen durchzusetzen. Darüber hinaus kann es öffentliche Erklärungen abgeben und dem Parlament berichten.

Für das Geschäftsjahr 1977 laufen drei größere Forschungsvorhaben, nämlich eine Studie über Personaldatenbanken, eine weitere über Kriminaldatenbanken und eine über Aspekte des Schutzes der Privatsphäre bei der Praxis der Personaleinstellung. Andere Forschungsthemen werden sein: Kreditinformation, Volkszählung, Presserat, medizinische Datenbanken, Verkauf durch Versandhäuser und per Telefon, medizinische Bescheinigungen, obligatorische Meldung von Kindesmißhandlung, Inkassopraktiken, Projekte der Bewährungshilfe und schließlich Methoden der Marktforschung.

In den ersten 18 Monaten seines Bestehens hat das Committee 1000 Beschwerden empfangen. Bis auf einen kleinen Rest konnte es alle Beschwerden zur Zufriedenheit der Beschwerdeführer aufklären. Die Tätigkeit ist gebührenfrei.

Seine bisherige Arbeit wird in der Öffentlichkeit als so erfolgreich angesehen, daß die Kommission für Gesetzreform erwägt, auch auf Bundesebene ein derartiges Gremium zu schaffen.

3.2.8 Neuseeland

In Neuseeland steht nach wie vor das geplante Kriminalinformationssystem[19]) L.E.I.S. (Law Enforcement Information System) im Blickpunkt der öffentlichen Diskussion. Die Vorstellung des Projekts, die eine lebhafte allgemeine Diskussion über den Schutz der Privatsphäre auslöste, hatte dazu geführt, daß der Datenschutz schon 1972 zum Wahlkampfthema wurde. Der damals von der Labour Party vorgelegte Entwurf eines Gesetzes zum Schutze der Privatsphäre sah einen Datenschutzbeauftragten mit weitreichenden Vollmachten, Registrierungspflicht für alle Datenbanken

[17]) Vgl. The Law Reform Commission, Annual Report 1976, herausgegeben von der Australischen Regierung

[18]) Vgl. „Introducing the Privacy Committee", D. West, Government Printer, New South Wales – 1976.

[19]) Vgl. III, 2.3.9.

und das Recht des Bürgers auf einen kostenlosen Ausdruck der über ihn gespeicherten Daten vor. Nach dem Wahlsieg der Labour Party hat die neue Regierung am 25. Juli 1975 dem Parlament drei Gesetzentwürfe vorgelegt, mit denen ein Schutz der Privatsphäre erzielt werden soll: Die Entwürfe eines Gesetzes über Abhöranlagen, eines Gesetzes über einen Datenschutzbeauftragten und eines Gesetzes über das Rechenzentrum Wanganui.

Der Gesetzentwurf über den Datenschutzbeauftragten gibt diesem, im Gegensatz zu dem erwähnten Entwurf, nur die Befugnis, Probleme der Privatsphäre zu untersuchen, dem Justizminister zu berichten und Empfehlungen über gesetzgeberische und Verwaltungsmaßnahmen zu geben. Die seinerzeit vorgesehenen weitreichenden Vollmachten sind, ebenso wie die geplante gesetzliche Garantie des Schutzes der Privatsphäre, weggefallen.

Das Rechenzentrum Wanganui bildet mit den geplanten 197 im ganzen Land aufgestellten Datenstationen die Basis für die Verwirklichung des Projektes L.E.I.S. Das betreffende Gesetz sieht für dieses Rechenzentrum einen besonderen Datenschutzbeauftragten vor. Er hat Beschwerden von Einzelpersonen nachzugehen und kann von sich aus Untersuchungen im Zusammenhang mit dem Betrieb des Rechenzentrums anstellen. Seine Untersuchungen sind nicht öffentlich, jedoch legt er dem Parlament einen Jahresbericht vor. Jedermann kann den Datenschutzbeauftragten einmal im Jahr um den Ausdruck der über ihn gespeicherten Informationen bitten; der Datenschutzbeauftragte kann die Auskunft verweigern, wenn sie eine Strafverfolgung beeinträchtigen würde.

Die Kritik an diesen Entwürfen bemängelt, daß mit dem bereits vorhandenen Ombudsman insgesamt vier Beauftragte für den Schutz der Privatsphäre nebeneinander bestünden (auch das Gesetz über Abhöranlagen sieht einen solchen vor), und daß der gesetzliche Schutz der Privatsphäre nach wie vor unzulänglich sei, obwohl computergestützte Informationssysteme u. a. im Bereich der Statistik, des Steuerwesens, der Wählerkartei, der Sozialversicherung und des Krankenhauswesens geplant seien.

3.3 Internationale und Supranationale Organisationen

3.3.1 Europarat

Die Rechtsabteilung des Europarats hat im Juli 1976 den Vorentwurf einer internationalen Konvention über Datenschutz vorgelegt. Diese geht inhaltlich zurück auf die Resolution (73) 22 über den Schutz des Persönlichkeitsrechts des einzelnen hinsichtlich elektronischer Datenbanken im privaten Bereich vom 26. 9. 1973 und die Resolution (74) 29 über den Schutz des Persönlichkeitsrechts des einzelnen hinsichtlich elektronischer Datenbanken im öffentlichen Bereich vom 20. 9. 1974[20]). Ein externes Kontrollorgan für den Datenschutz ist vorgesehen, jedoch fehlt nach wie vor die Einbeziehung des Schutzes der Gewaltenteilung.

Besonders ausführlich hat sich der Europarat mit der sog. grenzüberschreitenden Datenverarbeitung („transfrontier data flow") beschäftigt. Um auf diesem Gebiet, das ebenfalls in der geplanten Konvention geregelt werden soll, möglichst bald zu einem Konsens zu kommen, hat er im Januar 1977 den Bericht einer Expertengruppe vorgelegt; dieser enthält einen Überblick über die Regelungen, die in den Mitgliedsländern hinsichtlich grenzüberschreitender Datenverarbeitung bestehen oder geplant sind. Die in Aussicht genommene Konvention ist für die Bundesrepublik von besonderer Bedeutung, denn das BDSG regelt diese Materie nur in einem Einzelfall[21]).

3.3.2 Europäische Gemeinschaften (EG)

Auch die Organe der EG bemühen sich seit mehreren Jahren um eine gemeinsame europäische Entwicklung auf dem Gebiet des Datenschutzes. Aufgrund des Berichts seines Rechtsausschusses vom 19. 2. 1975[22]) hat das Europäische Parlament am 8. 4. 1976 eine Entschließung verabschiedet, mit der die EG-Kommission aufgefordert wird[23]), Informationen zu sammeln im Hinblick auf den Entwurf einer Direktive für den Schutz des Persönlichkeitsrechts. Die Kommission hat eine Sachverständigengruppe eingesetzt mit dem Auftrag, Material zum Schutz des Persönlichkeitsrechts als Grundlage für die Ausarbeitung gemeinschaftlicher Rechtsvorschriften zu sammeln.

Am 10. 1. 1977 hat der Rechtsausschuß des Europäischen Parlaments einen weiteren Bericht („Arbeitsdokument") vorgelegt[24]) „über einzuleitende oder fortzuführende Tätigkeiten der Gemeinschaften im Hinblick auf den Schutz der Rechte des einzelnen gegenüber dem technischen Forschritt im Bereich der automatischen Datenverarbeitung".

3.3.3 OECD

Ebenso wie Europarat und EG ist die OECD außerordentlich an Fragen des Datenschutzes in-

[20]) Vgl. IV, 2.2.1.

[21]) § 11 Satz 3 BDSG.

[22]) Vgl. IV, 2.2.1.

[23]) ABL. 100/27.

[24]) PE 47 228.

teressiert. Bereits seit einiger Zeit besteht eine ad-hoc-Arbeitsgruppe („Data-Bank-Panel"), die sich vorwiegend mit Datenschutzfragen im Bereich der grenzüberschreitenden Datenverarbeitung befaßt. Mit dieser Arbeitsgruppe habe ich Fragen des Zugriffsrechts der Parlamente auf Verwaltungsdaten sowie der Harmonisierung des Datenschutzrechts innerhalb der OECD-Mitgliedstaaten und im grenzüberschreitenden Datenverkehr erörtert. Die Erkenntnisse der Arbeitsgruppe sind in einem Bericht zusammengefaßt, der am 15. November 1976 vorgelegt wurde und die Grundlage für die weiteren Beratungen innerhalb des Direktorats für Naturwissenschaft, Technologie und Industrie/Gruppe Computer-Anwendung bilden soll. Er hat den Titel „The Transborder Movement and Protection of Data — Principles and Guidelines"[25]). Der Bericht ist gleichzeitig das Arbeitspapier für ein unter diesem Thema für 1977 geplantes Symposium.

[25]) DSTI/CUG/76.36, 30.244.

4. ERFAHRUNGEN IM BERICHTSZEITRAUM

4. Erfahrungen im Berichtszeitraum

Aufgrund von Eingaben, stichprobeartigen Kontrollen bei Dienstreisen und der Auswertung von mir vorgelegten Berichten sowie von Zeitungsmeldungen sind mir eine Reihe von Vorfällen bekannt geworden, in denen es sich als notwendig erwies, zu prüfen, ob und inwieweit ein Verstoß gegen Datenschutzbestimmungen vorlag. Aus diesen von mir untersuchten Vorgängen habe ich einige herausgegriffen, weil ich sie für symptomatisch halte und die dabei in Erscheinung getretenen Gefahren für die Persönlichkeitsrechte des Bürgers bei den Bestrebungen um einen verbesserten Datenschutz in die Diskussion einbezogen werden sollten.

4.1 Datenschutz bei Versicherungen

In einer Eingabe unterrichteten mich zwei Versicherungsvertreter davon, daß sie nach Auflösung ihrer Verträge mit einer privaten Versicherungsgesellschaft trotz Bewerbungen bei zahlreichen anderen Gesellschaften, darunter auch einer der Aufsicht des Landes unterstehenden Anstalt des öffentlichen Rechts, keine neue Anstellung fanden. Erst durch intensive Nachforschungen erfuhren sie, daß die ablehnenden Bescheide auf — wie sich später ergab — unrichtige Auskünfte zurückzuführen waren, die von einer gemeinsamen Auskunftsstelle der Versicherungswirtschaft und der Bausparkassen herrührten. Von ihr werden Informationen über Vertreter im Außendienst zentral gespeichert und den Mitgliedern auf Anforderung übermittelt. Die Meldung, die die Versicherungsgesellschaften beim Ausscheiden eines Vertreters machen, enthält u. a. den Kündigungsgrund, das polizeiliche Führungszeugnis (Strafvermerke? ja/nein), zivilrechtliche Vollstrekkungsmaßnahmen, Beanstandungen der Vertretertätigkeit, Ansprüche der Gesellschaft gegen den Vertreter, Umsätze und Stornierungen. Es ist festgelegt, daß „alle Auskünfte ... streng vertraulich und nur zur eigenen Unterrichtung bestimmt (sind und) weder ganz noch teilweise oder auch nur andeutungsweise jenen zur Kenntnis gebracht werden (dürfen), auf die sich die Auskunft bezieht". Entsteht „durch eine Indiskretion ein Schaden", so kann „das dafür verantwortliche Mitglied regreßpflichtig" gemacht werden.

Der Vorgang zeigt exemplarisch, welche Bedeutung die Kontrollrechte für den Betroffenen haben können. Der bisher geübten Praxis ist er praktisch schutzlos ausgeliefert. Das kartellähnliche Zusammenwirken der Versicherungsgesellschaften kann dazu führen, daß der betroffene Vertreter auf Dauer seinen Beruf nicht mehr ausüben kann. Schreibfehler, Übermittlungsfehler und Personenverwechslungen sind ebensowenig auszuschließen wie schikanöse Falschmeldungen.

Ich habe die betreffende Anstalt des öffentlichen Rechts auf diesen Umstand hingewiesen. Zwar werden die Vorgänge, da sie bisher manuell ablaufen, vom HDSG nicht erfaßt. Die Einschränkung des Datenschutzes auf die maschinelle Datenverarbeitung wird jedoch mit dem Inkrafttreten des Bundesdatenschutzgesetzes und, soweit absehbar, auch des neuen Hessischen Datenschutzgesetzes wegfallen. Danach wird der einzelne auch in manuell geführten Dateien für seine Daten Auskunfts- und Berichtigungsrechte haben.

Die genannte Anstalt will jetzt auf eine Revision der bisher geübten Praxis hinwirken. Dabei sollte beachtet werden, daß eine Mitteilung an eine zentrale Auskunftsstelle nur erfolgen darf, wenn der Betroffene seine Einwilligung erklärt hat. Der Inhalt der Mitteilung ist ihm unverzüglich bekanntzugeben. Nur so kann der Betroffene vor Nachteilen infolge falscher oder nicht beweisbarer Angaben geschützt werden.

4.2 Datenschutz bei Umfragen

Auch im Berichtszeitraum 1976/77 hat sich gezeigt, daß der Datenschutz bei Umfragen noch eine Reihe von Problemen aufwirft, die gelöst werden müssen, wenn Gefährdungen für das Persönlichkeitsrecht der Teilnehmer vermieden werden sollen. Ein Beispiel mag das verdeutlichen.

Im März 1976 teilte der Bundesminister für Bildung und Wissenschaft dem Hessischen Kultusminister mit, daß er mit Hilfe einer schriftlichen Befragung von Schülern, die nicht nach dem Bundesausbildungsförderungsgesetz (BAföG) gefördert werden, aber zum prinzipiell antragsberechtigten Personenkreis gehören, Erkenntnisse über das Ausschöpfungsverhalten gewinnen und das BAföG-Berechnungs- und -Prognosemodell verbessern wolle. Da unter anderem auch 2000 hessische Schüler befragt werden sollten, wurde der Kultusminister gebeten zu genehmigen, daß die dafür ausgewählten hessischen Ausbildungsanstalten dem mit der Durchführung beauftragten privaten Marktforschungsinstitut die entsprechenden Adressen direkt übermitteln. Der Bundesminister für Bildung und Wissenschaft versi-

cherte, daß gegen eine mißbräuchliche Verwendung der Daten Vorsorge getroffen werde. Das Befragungsinstitut liefere der mit der weiteren Bearbeitung beauftragten Gesellschaft für Mathematik und Datenverarbeitung (GMD) nur die zusammengefaßte Auswertung in EDV-aufbereiteter Form ohne individualisierende Merkmale; die Adressen würden von dem Befragungsinstitut vernichtet.

Auf Wunsch des Kultusministers habe ich zu diesem Projekt Stellung genommen und zur Präzisierung und Verbesserung des Datenschutzes unter anderem angeregt:

„1. Die Befragung erfolgt auf freiwilliger Grundlage. Hierauf müssen die Befragten unmißverständlich hingewiesen werden. ...

2. Die vertrauliche Behandlung der Angaben durch das erhebende Institut ist den Betroffenen besonders zuzusichern.

3. Die... abzuliefernden Ergebnisse müssen soweit anonymisiert sein, daß Rückschlüsse auf Angaben einzelner Befragter nicht möglich sind."

Der Kultusminister hat diese Anforderungen zum Inhalt seiner Genehmigung gemacht.

Meine Feststellungen haben ergeben, daß bei der Durchführung der Befragung in einer Reihe von Punkten, teilweise unter Mißachtung der erwähnten Auflagen, der Datenschutz nicht ausreichend berücksichtigt wurde:

1. Ein ausdrücklicher Hinweis auf die Freiwilligkeit der Beantwortung findet sich zwar in einem an die Schulleitungen gerichteten Schreiben des Instituts, nicht aber in den Schreiben, die an die befragten Schüler und ihre Eltern gerichtet worden sind.

2. Anstelle einer ausdrücklichen Zusicherung einer vertraulichen Behandlung der Angaben durch das Institut findet sich in dessen Briefen die Aussage, „der Fragebogen (sei) vollständig anonym". Diese Behauptung ist falsch. Zwar enthält der Fragebogen kein direktes Indentifizierungsmerkmal, doch ergeben sich aus den einzelnen Angaben, wie Postleitzahl des Schulortes, Postleitzahl des Wohnortes, Anzahl, Alter und Vornamen der Geschwister, durchaus Möglichkeiten, die Person des Befragten zu bestimmen.

3. Der Kultusminister hatte die „Überlassung der ... benötigten Adressen" genehmigt. Gleichwohl hat das beauftragte Marktforschungsinstitut die Schulleitungen unter Berufung auf den Erlaß um „Ablichtungen" bzw. „Überlassung von Schülerkarteien" gebeten. In vielen Schulen enthalten die Schülerkarteien aber auch die Namen der Eltern, teilweise auch deren Beruf und das Religionsbekenntnis des Schülers sowie weitere für die Schulverwaltung wesentliche Daten. Es muß angenommen werden, daß zumindest ein Teil der Schulen Ablichtungen der vollständigen Schülerkarteien geliefert haben. Weder der Kultusminister noch der Bundesminister für Bildung und Wissenschaft haben darin einen Anlaß zur Intervention gesehen.

Der Vorgang zeigt, daß sowohl die beteiligten Behörden als auch das Marktforschungsinstitut die sich aus den Datenschutzforderungen ergebenden Anforderungen zugunsten geringfügiger Arbeitserleichterungen übergehen. Die Institute sind vor allem anderen daran interessiert, die benötigten Adressen zu erhalten und bei den Fragebögen eine hohe Rücklaufquote zu erzielen. Daran wird der gesamte Verfahrensablauf ausgerichtet. Die Kultusverwaltung erteilt zwar, was anzuerkennen ist, besondere Auflagen zur Gewährleistung des Datenschutzes, kontrolliert aber, auch bei gegebenem Anlaß, nicht deren Einhaltung.

Daraus ergeben sich folgende Forderungen:

1. Soweit die Verwaltung gespeicherte personenbezogene Daten Außenstehenden zugänglich macht, sollen die zu überlassenden Daten so präzis wie möglich umschrieben werden. Zugleich ist anzuordnen, daß keine anderen Daten übermittelt werden dürfen. Die Aufsichtsbehörden sollen die Einhaltung dieser Bestimmung und aller anderen Datenschutzauflagen kontrollieren, soweit dafür nach den Umständen des Einzelfalles Anlaß besteht.

2. Bei freiwilligen Befragungen müssen die Teilnehmer über den Zweck der Umfrage und den Schutz ihrer Daten klar, umfassend und zutreffend unterrichtet werden. Dem entsprechen die §§ 7, 11 und 17 E. Soweit öffentliche Stellen private Institute mit Erhebungen beauftragen, ist die Einhaltung dieser Grundsätze vertraglich zu sichern. Dasselbe muß gelten, wenn die Verwaltung Dritten für Vorhaben der wissenschaftlichen oder angewandten Forschung Daten überläßt. Um die Einhaltung des Datenschutzes prüfen zu können, muß sich die Verwaltung die kompletten Erhebungsunterlagen und einen Ablaufplan vorlegen lassen.

4.3 Datenschutz in der Verwaltungspraxis

Wie die Presse berichtete, sind bei einer süddeutschen Allgemeinen Ortskrankenkasse (AOK) sensitive Diagnosedaten durch vorübergehend beschäftigte Aushilfsangestellte ausgewertet wor-

den. Die dadurch mögliche Gefährdung des Datenschutzes von Patienten hat mich veranlaßt, den Stand der EDV-Anwendung bei den hessischen AOK zu überprüfen.

Nach meinen Feststellungen ist nicht zu befürchten, daß es hier zu einem ähnlichen Vorfall kommen könnte: Zwar wird gegenwärtig ein Rechenzentrum des Landesverbandes der Allgmeinen Ortskrankenkassen in Hessen, in welchem später auch Diagnose-Daten ausgewertet werden sollen, aufgebaut. Aber bereits jetzt untersucht eine Arbeitsgruppe die mit der Auswertung von Diagnose-Daten verbundenen Probleme der ärztlichen Schweigepflicht und des Datenschutzes. Ich konnte feststellen, daß auch während der Aufbauphase des Rechenzentrums Datenschutz- und Datensicherheitsmaßnahmen beachtet werden. Der Datenschutzbeauftragte wird über die Entwicklung seitens der AOK auf dem laufenden gehalten.

Auch in Hessen sind aber trotz des bereits über sechsjährigen Bestehens des Hessischen Datenschutzgesetzes vergleichbare Fälle der Gefährdung des Datenschutzes noch möglich. Das zeigen meine Feststellungen bei stichprobenartigen Kontrollen verschiedener Stellen der Verwaltung sowie von Rechenzentren:

In einer kleineren Stadtverwaltung in Mittelhessen wurden bei der Umstellung des Einwohnermeldewesens auf die EDV zur Übertragung der in der Meldekartei befindlichen Daten — unter denen sich auch empfindliche Daten, wie z. B. „Verlust des Wahlrechts" befinden — vorübergehend Hilfskräfte eingestellt. Obwohl diese bei ihrer Tätigkeit zwangsläufig auch empfindliche Daten zur Kenntnis nehmen mußten, waren sie nicht auf das Datengeheimnis (§ 3 HDSG) und die entsprechende Schweigepflicht hingewiesen bzw. formell verpflichtet worden.

Die von der Stadtverwaltung vertretene Auffassung, das Hessische Datenschutzgesetz sei auf diesen Fall nicht anwendbar, ist unzutreffend: Nicht nur bezieht § 3 HDSG die Datenerfassung in das Datengeheimnis ein, sondern auch die Formulierung von § 1 HDSG, „der Datenschutz erfaßt alle für Zwecke der maschinellen Datenverarbeitung erstellten Unterlagen . . ." macht zweifelsfrei deutlich, daß die Erfassung von Einwohnerdaten auf Datenträgern unter das Datenschutzgesetz fällt.

Daß Datenschutzprobleme nicht nur bei der Erfassung, sondern auch hinsichtlich der Vernichtung von Daten entstehen können, zeigt ein vergleichsweise harmloser Fall aus einer anderen Gemeinde: Dort waren nicht mehr gebrauchte EDV-Unterlagen — es handelte sich um einen vom zuständigen KGRZ erstellten Teil der Einwohnerbestandsliste mit unverschlüsselten Personendaten — von der Gemeindeverwaltung an einen Kindergarten als Schmierpapier weitergegeben worden. Auch hier waren — wie aus der Antwort des Ministers des Innern auf eine im Landtag erhobene Anfrage[1]) zu entnehmen ist — die bestehenden gesetzlichen Vorschriften den zuständigen Bediensteten nicht bekannt oder bewußt.

Aber nicht nur im behördeninternen Umgang mit Daten bleiben Datenschutzvorschriften oft unbeachtet; nicht minder bedenklich ist im kommunalen Bereich die z. T. recht großzügig gehandhabte Weitergabe von Einwohnerdaten an Dritte. Wenn konkrete Schädigungen von Bürgern bisher nicht bekannt geworden sind, so ist dies nicht das Verdienst der für die Datenweitergabe verantwortlichen Kommunalverwaltungen: Bei Stichproben des Datenschutzbeauftragten in den verschiedenen Kommunalen Gebietsrechenzentren (KGRZ) wurde festgestellt, daß von 13 Gemeinden Aufträge vorlagen, Adressenlisten von Haushaltungsvorständen, von männlichen Personen, von Verheirateten, von allen Ausländern oder den Angehörigen bestimmter Nationalitäten bzw. religiöser Bekenntnisse, von einzelnen Jahrgängen usw. an Privatfirmen — Versicherungsvertreter, Banken, Fernakademien, Adressenverlage, Marktforschungs-Unternehmen und dergleichen — zu liefern. Bei einer Durchsicht der bei den KGRZ vorliegenden Bearbeitungsaufträge ergab sich die Vermutung, daß in einer Reihe weiterer Datenanforderungen von Mitgliedsgemeinden des KGRZ, deren Zweck im Auftrag nicht angegeben ist, die Absicht bestand, die vom KGRZ gelieferten Ausdrucke von Einwohnerlisten an Dritte weiterzugeben.

Diese Praxis ist mit dem Datenschutz nicht zu vereinbaren. Schon nach den bisher gültigen Verwaltungsvorschriften zum Hessischen Meldegesetz (VVMeldeG) sind Sammelauskünfte nur zulässig, wenn ein öffentliches Interesse nachgewiesen ist; darüber hinaus muß ein berechtigtes Interesse nachgewiesen sein, wenn „Tag und Ort der Geburt, Beruf, Familienstand und Staatsangehörigkeit" gefordert werden. Auch nach der Regelung des VVMeldeG (Abschnitt IV F Abs. 2 d) ist die Erteilung der Auskunft zu versagen, wenn „aus der Auskunftserteilung eine Gefahr für . . . die persönliche Freiheit erwachsen könnte". Diese Einschränkung zusammen mit der Voraussetzung des öffentlichen (berechtigten) Interesses lassen es als sehr zweifelhaft erscheinen, ob die von den Gemeinden veranlaßten Weitergaben von Einwohnerdaten befugt waren. Aus der Sicht des Datenschutzes sind sie in jedem Falle zu beanstanden: Der Datenschutzbeauftragte hat bereits in

[1]) LT-Drucks. 8/2847 vom 22. 7. 1976 zu LT-Drucks. 8/2465.

mehreren Tätigkeitsberichten[2]) kritisiert, daß personenbezogene Daten, die der Behörde für einen bestimmten Zweck gegeben wurden, von dieser ohne Wissen und Zustimmung des Betroffenen an Dritte, insbesondere Privatfirmen weitergegeben wurden. Dabei handelt es sich um einen Eingriff in das Recht des Bürgers, über die Verwendung von Informationen über seine Person selbst zu bestimmen[3]).

In zunehmender Zahl wenden sich aber auch Gemeinden an mich, bevor sie Wünsche auf Datenweitergabe erfüllen und fragen an, ob dagegen aus Datenschutzgründen Bedenken bestehen. Wiederholt handelte es sich um die Weitergabe bestimmter Daten an Adressbuchverlage. Wie schon in früheren Tätigkeitsberichten ausgeführt wurde[4]) sollten Einwohnerdaten („Sammelauskünfte") nur weitergegeben werden, wenn die Weitergabe im öffentlichen Interesse liegt und der Bürger das Recht hat, seine Daten zu sperren.

Eine ähnliche Praxis wie im Einwohnerwesen ist auch im Bauwesen zu beobachten: Hier ist allerdings den kommunalen Baubehörden kein Vorwurf zu machen, da sich die Praxis im Einklang mit den Anweisungen der obersten Aufsichtsbehörde, des Innenministers, befindet. Trotzdem bedarf die jetzige Praxis im Lichte der inzwischen vorliegenden Erfahrungen des Datenschutzes einer Überprüfung.

Zur Frage der Unterrichtung von Verlagen für Bauten-Nachweise über erteilte Baugenehmigungen durch die unteren Bauaufsichtsbehörden heißt es im Erlaß des Hessischen Innenministers vom 14. 8. 1970[5]) unter Ziffer 2: „Das Einverständnis der Bauherren mit der Unterrichtung der Verlage ist nicht erforderlich. Objektive Nachteile für sie sind nicht zu erwarten". Unter Bezugnahme auf diesen Erlaß betont ein weiterer Erlaß des Innenministers vom 11. 3. 1975[6]), daß wegen des zwischen dem antragstellenden Bürger und der Behörde bestehenden Rechts- und Vertrauensverhältnisses die Behörde verpflichtet sei, die mit dem Bauantrag „verbundenen Angaben und Mitteilungen vertraulich zu behandeln". Weiter heißt es: „Eine Veröffentlichung der Bauanträge ... ist somit weder notwendig noch möglich". Allerdings könne aus Gründen des „Interesses an einem verstärkten Wettbewerb innerhalb der Bauwirtschaft" ein öffentliches Interesse für die Datenweitergabe an einen begrenzten Kreis von Interessenten, nämlich die Verlage für Bauten-Nachweise und die interessierten Wirtschaftskreise, angenommen werden.

Ohne daß dieses öffentliche Interesse in Zweifel gezogen werden soll — und bei Anerkennung der Bemühung um eine abgewogene Regelung bezüglich der Weitergabe von Daten aus Baugenehmigungen — steht diese Praxis nicht im Einklang mit den inzwischen auf anderen Gebieten im Interesse des Datenschutzes vorgenommenen Einschränkungen[7]). Trotz ähnlicher Zielsetzung, nämlich Förderung des Wettbewerbs im Bereiche der Wirtschaft, dürfen weder die Standesämter noch das Kraftfahrtbundesamt bzw. die Kfz.-Zulassungsstellen Daten ohne Zustimmung des betroffenen Bürgers für gewerbliche Zwecke an Privatfirmen weitergeben.

Auch wenn bisher eine Mehrheit der Bürger keine Einwendungen gegen die Weitergabe ihrer Daten an interessierte Wirtschaftskreise erhoben hat — wie dies hinsichtlich der Mitteilung von Baugenehmigungen offenbar zutrifft — ist zum Schutz des Persönlichkeitsrechts zu fordern, daß eine Weitergabe nur unter der Voraussetzung erfolgt, daß der Betroffene bei Antragstellung ausdrücklich zugestimmt hat. Unter den gegebenen Umständen kann jedenfalls das Interesse an der Wirtschaftsförderung gegenüber dem Schutz des Persönlichkeitsrechts nicht vorrangig sein.

Die stichprobenweise Überwachung des Datenschutzes hat gezeigt, daß bei einer großen Anzahl von Kommunalverwaltungen Unsicherheit über die Anwendung des Hessischen Datenschutzgesetzes und seine praktischen Auswirkungen auf die Verwaltung besteht. Ich halte es deshalb für erforderlich, daß die zuständige Aufsichtsbehörde auf eine Regelung des Datenschutzes entsprechend den im Hessischen Datenverarbeitungs-Verbund geltenden Datenschutz-Bestimmungen hinwirkt.

Wiesbaden, den 10. März 1977

Professor Dr. S. Simitis

---

[2]) II, 1.3.2; III, 1.5.6; IV, 1.6, 4.7.8 und 5.1.6; V, 4.5.2.

[3]) Vgl. III, 1.5.6.

[4]) III, 1.5.6; IV, 4.7.8; V, 4.5.

[5]) VA 4 — 64 a 02/02 — 9/70, StAnz. 36/1970, S. 1741.

[6]) VA 4 — 64 a 06/01 — 9/75, StAnz. 13/1975, S. 573.

[7]) Vgl. IV, 4.7.8; V, 4.5.2.1 und 4.5.5.

INHALTSÜBERSICHT ZUM ENTWURF FÜR EIN HESSISCHES DATENSCHUTZGESETZ

Anlage zu Abschnitt 2

GEGENÜBERSTELLUNG DES ENTWURFS FÜR EIN HESSISCHES DATENSCHUTZGESETZ MIT DEM BUNDESDATENSCHUTZGESETZ

Entwurf HDSG	BDSG
Erster Abschnitt **Allgemeine Vorschriften**	
§ 1 Aufgabe des Datenschutzes Aufgabe des Datenschutzes ist es, 1. den Bürger vor einer Beeinträchtigung durch die Verarbeitung personenbezogener Daten zu schützen und 2. das verfassungsmäßige Gefüge des Staates, insbesondere der Verfassungsorgane des Landtags und der Organe der kommunalen Selbstverwaltung untereinander und zueinander vor einer Veränderung infolge der automatisierten Datenverarbeitung zu bewahren.	§ 1 Aufgabe und Gegenstand des Datenschutzes (1) Aufgabe des Datenschutzes ist es, durch den Schutz personenbezogener Daten vor Mißbrauch bei ihrer Speicherung, Übermittlung, Veränderung und Löschung (Datenverarbeitung) der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.
§ 2 Geltungsbereich (1) Dieses Gesetz gilt 1. für die Behörden und sonstigen öffentlichen Stellen des Landes einschließlich der Gerichte, 2. für die Behörden und sonstigen öffentlichen Stellen der Gemeinden und Gemeindeverbände und deren Vereinigungen, 3. für sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts, wenn sie personenbezogene Daten in Dateien verarbeiten oder aus Dateien übermitteln.	§ 1 Aufgabe und Gegenstand des Datenschutzes (2) Dieses Gesetz schützt personenbezogene Daten, die 1. von Behörden oder sonstigen öffentlichen Stellen (§ 7), 2. von natürlichen oder juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts für eigene Zwecke (§ 22), 3. von natürlichen oder juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts geschäftsmäßig für fremde Zwecke (§ 31) in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden. Für personenbezogene Daten, die nicht zur Übermittlung an Dritte bestimmt sind und in nicht automatisierten Verfahren verarbeitet werden, gilt von den Vorschriften dieses Gesetzes nur § 6.
Für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, gelten nur § 4, § 6 Abs. 1, §§ 14 bis 16 und 20 bis 25.	§ 7 Anwendungsbereich (1) Die Vorschriften dieses Abschnittes gelten für Behörden und sonstige öffentliche Stellen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie für Vereinigungen solcher Körperschaften, Anstalten und Stiftungen. Für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, gelten von den Vorschriften dieses Abschnittes jedoch nur die §§ 15 bis 21. (2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die Vorschriften dieses Abschnittes mit Ausnahme der §§ 15 bis 21 auch für 1. Behörden und sonstige öffentliche Stellen der Länder, der Gemeinden und Gemeindeverbände und der son-

Entwurf HDSG

BDSG

stigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen, soweit sie Bundesrecht ausführen.

2. Behörden und sonstige öffentliche Stellen der Länder, soweit sie als Organe der Rechtspflege tätig werden, ausgenommen in Verwaltungsangelegenheiten.

Für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen und soweit sie die Voraussetzungen von Satz 1 Nr. 1 erfüllen, gelten die Vorschriften dieses Abschnittes nicht.

§ 22 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie geschützte personenbezoge Daten als Hilfsmittel für die Erfüllung ihrer Geschäftszwecke oder Ziele verarbeiten. Sie gelten mit Ausnahme der §§ 28 bis 30 nach Maßgabe von Satz 1 auch für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, soweit sie die Voraussetzungen von § 7 Abs. 1 Satz 1 oder § 7 Abs. 2 Satz 1 Nr. 1 erfüllen.

§ 31 Anwendungsbereich

(1) Für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts sowie für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, soweit sie die Voraussetzungen von § 7 Abs. 1 Satz 1 oder § 7 Abs. 2 Satz 1 Nr. 1 erfüllen, gelten

1. die §§ 32 bis 35, soweit diese Stellen geschäftsmäßig geschützte personenbezogene Daten zum Zweck der Übermittlung speichern und übermitteln; dabei ist es unerheblich, ob die Daten vor der Übermittlung verändert werden,
2. § 36, soweit diese Stellen geschäftsmäßig geschützte personenbezogene Daten zum Zweck der Veränderung speichern, sie derart verändern, daß diese Daten sich weder auf eine bestimmte Person beziehen noch eine solche erkennen lassen (anonymisieren), und sie in dieser Form übermitteln,
3. § 37, soweit diese Stellen geschäftsmäßig geschützte personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten.

Für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts gelten außerdem die §§ 38 bis 40. Satz 2 gilt nicht für juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, soweit diese Personen oder Personenvereinigungen geschäftsmäßig geschützte personenbezogene Daten im Auftrag von Behörden oder

Entwurf HDSG

(2) Soweit die Datenverarbeitung frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse betrifft, gelten anstelle der §§ 5, 7 bis 9, 11 und 12 dieses Gesetzes die §§ 23 und 24 Abs. 1 sowie §§ 25 bis 27 des Bundesdatenschutzgesetzes (BDSG) vom 27. Januar 1977 (Bundesgesetzbl. I S. 201).

(3) Dieses Gesetz gilt nicht für die Anstalt des öffentlichen Rechts „Hessischer Rundfunk", soweit sie personenbezogene Daten ausschließlich zu eigenen publizistischen Zwecken verarbeitet; § 15, §§ 20 bis 22 Abs. 1 und § 25 bleiben unberührt.

§ 3 Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Im Sinne dieses Gesetzes ist Verarbeiten (Verarbeitung) das Speichern, das Verändern, das Übermitteln, das Sperren und das Löschen personenbezogener Daten.

(3) Im Sinne dieses Gesetzes ist

1. Speichern (Speicherung): Das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verwendung,
2. Verändern (Veränderung): Das inhaltliche Umgestalten gespeicherter Daten,
3. Übermitteln (Übermittlung): Das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an Dritte in der Weise, daß die Daten durch die speichernde Stelle weitergegeben oder zur Einsichtnahme, namentlich zum Abruf bereitgehalten werden,
4. Sperren (Sperrung): Das Verhindern weiterer Verarbeitung oder sonstiger Nutzung gespeicherter Daten,
5. Löschen (Löschung): Das Unkenntlichmachen gespeicherter Daten,

ungeachtet der dabei angewendeten Verfahren.

(4) Im Sinne dieses Gesetzes ist

1. speichernde Stelle jede der in § 2 Abs. 1 genannten Stellen, die Daten für sich selbst speichert oder durch andere speichern läßt,
2. Dritter jede Person oder Stelle außerhalb der speichernden Stelle, mit Ausnahme des Betroffenen sowie derjenigen Personen und Stellen, die in den Fällen der Nummer 1 im Geltungsbereich des Grundgesetzes im Auftrag tätig werden,

BDSG

sonstigen öffentlichen Stellen als Dienstleistungsunternehmen verarbeiten; § 8 Abs. 3 bleibt unberührt.

§ 7 Anwendungsbereich

(3) Abweichend von den Absätzen 1 und 2 gelten anstelle der §§ 9 bis 14 die §§ 23 bis 27 entsprechend, soweit die Datenverarbeitung frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse betrifft.

§ 1 Aufgabe und Gegenstand des Datenschutzes

(3) Dieses Gesetz schützt personenbezogene Daten nicht, die durch Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films ausschließlich zu eigenen publizistischen Zwecken verarbeitet werden; § 6 Abs. 1 bleibt unberührt.

§ 2 Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Im Sinne dieses Gesetzes ist

1. Speichern (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verwendung,
2. Übermitteln (Übermittlung) das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an Dritte in der Weise, daß die Daten durch die speichernde Stelle weitergegeben oder zur Einsichtnahme, namentlich zum Abruf bereitgehalten werden,
3. Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter Daten,
4. Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten,

ungeachtet der dabei angewendeten Verfahren.

(3) Im Sinne dieses Gesetzes ist

1. speichernde Stelle jede der in § 1 Abs. 2 Satz 1 genannten Personen oder Stellen, die Daten für sich selbst speichert oder durch andere speichern läßt,
2. Dritter jede Person oder Stelle außerhalb der speichernden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die in den Fällen der Nummer 1 im Geltungsbereich dieses Gesetzes im Auftrag tätig werden,
3. eine Datei eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden kann, ungeachtet der dabei angewendeten Verfahren; nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie

Entwurf HDSG

3. eine Datei eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden kann, ungeachtet der dabei angewendeten Verfahren; nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

§ 4 Datengeheimnis

(1) Bedienstete der in § 2 Abs. 1 genannten Stellen, die bei der Datenverarbeitung beschäftigt sind, dürfen personenbezogene Daten zu keinem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck verarbeiten, bekanntgeben, zugänglich machen oder sonst nutzen.

(2) Das gleiche gilt für Personen, die bei der Datenverarbeitung beschäftigt sind, wenn Daten im Auftrag der in § 2 Abs. 1 genannten Stellen verarbeitet werden.

§ 5 Rechte des Betroffenen

Jeder hat nach Maßgabe dieses Gesetzes für die zu seiner Person gespeicherten Daten ein unverzichtbares Recht auf

1. Auskunft,
2. Berichtigung, wenn die Daten unrichtig sind,
3. Sperrung der Übermittlung an Stellen außerhalb des öffentlichen Bereichs,
4. Sperrung, wenn sich weder die Richtigkeit noch die Unrichtigkeit der Daten feststellen läßt oder wenn die Speicherung nachträglich unzulässig geworden ist,
5. Löschung, wenn die Speicherung unzulässg ist.

§ 6 Verantwortlichkeit für die Datenverarbeitung

(1) Die in § 2 Abs. 1 genannten Stellen haben den Datenschutz auch dann zu gewährleisten, wenn sie personenbezogene Daten durch andere Personen oder Stellen verarbeiten lassen.

(2) Der Schaden, der durch eine unzulässige Datenverarbeitung oder durch die Verarbeitung unrichtiger Daten entsteht, ist wieder gutzumachen. Der Geschädigte kann

BDSG

durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

§ 5 Datengeheimnis

(1) Den im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Personen oder Stellen bei der Datenverarbeitung beschäftigten Personen ist untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen.

(2) Diese Personen sind bei der Aufnahme ihrer Tätigkeit nach Maßgabe von Absatz 1 zu verpflichten. Ihre Pflichten bestehen auch nach Beendigung ihrer Tätigkeit fort.

§ 4 Rechte des Betroffenen

Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft über die zu seiner Person gespeicherten Daten,
2. Berichtigung der zu seiner Person gespeicherten Daten, wenn sie unrichtig sind,
3. Sperrung der zu seiner Person gespeicherten Daten, wenn sich weder deren Richtigkeit noch deren Unrichtigkeit feststellen läßt oder nach Wegfall der ursprünglich erfüllten Voraussetzungen für die Speicherung,
4. Löschung der zu seiner Person gespeicherten Daten, wenn ihre Speicherung unzulässig war oder – wahlweise neben dem Recht auf Sperrung – nach Wegfall der ursprünglich erfüllten Voraussetzungen für die Speicherung.

§ 8 Verarbeitung personenbezogener Daten im Auftrag

(1) Die Vorschriften dieses Abschnittes gelten für die in § 7 Abs. 1 und 2 genannten Stellen auch insoweit, als personenbezogene Daten in deren Auftrag durch andere Personen oder Stellen verarbeitet werden. In diesen Fällen ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen (§ 6 Abs. 1) sorgfältig auszuwählen.

Entsprechende Regelung fehlt.

Entwurf HDSG

auch Ersatz des ihm entstandenen Schadens in Geld verlangen; die Ersatzpflicht umfaßt den Schaden, der nicht Vermögensschaden ist.

(3) Die Schadenersatzpflicht nach Abs. 2 besteht nicht, soweit die in § 2 Abs. 1 genannten Stellen am Privatrechtsverkehr teilnehmen.

(4) Die Verpflichtung nach Abs. 2 trifft die in § 2 Abs. 1 genannte Gebietskörperschaft oder juristische Person des öffentlichen Rechts, die nach Abs. 1 den Datenschutz zu gewährleisten hat.

Zweiter Abschnitt
Vorschriften für die Datenverarbeitung

§ 7 Datenspeicherung und -veränderung

(1) Das Speichern und das Verändern personenbezogener Daten ist zulässig, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgabe erforderlich ist.

(2) Werden personenbezogene Daten beim Betroffenen erfaßt, ist er darüber zu belehren, aufgrund welcher Rechtsvorschrift er zur Auskunft verpflichtet ist. Besteht keine Auskunftspflicht, ist er darüber zu belehren, daß die Datenerfassung und weitere Verarbeitung nur mit seiner Einwilligung zulässig ist, daß ihm aus einer Verweigerung der Einwilligung keine Rechtsnachteile entstehen und daß die Verweigerung weder gespeichert noch in anderer Weise erfaßt wird.

(3) Die Einwilligung bedarf der Schriftform, wenn nicht wegen besonderer Umstände eine andere Form angemessen ist. Gegenstand, Inhalt und Umfang der erlaubten Verarbeitung, insbesondere die Datenarten, die Adressaten der Übermittlung, der Verwendungszweck und die Dauer der Aufbewahrung sind in der Einwilligungserklärung klar und verständlich zu bezeichnen.

§ 8 Datenübermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stellen ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgabe erforderlich ist.

(2) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden sind, dürfen vom Empfänger nur mit Einwilligung des Betroffenen weiter übermittelt werden; § 7 Abs. 2 und 3 sind entsprechend anzuwenden.

BDSG

§ 3 Zulässigkeit der Datenverarbeitung

Die Verarbeitung personenbezogener Daten, die von diesem Gesetz geschützt werden, ist in jeder ihrer in § 1 Abs. 1 genannten Phasen nur zulässig, wenn

1. dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
2. der Betroffene eingewilligt hat.

Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist; wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen.

§ 9 Datenspeicherung und -veränderung

(1) Das Speichern und das Verändern personenbezogener Daten ist zulässig, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist.

(2) Werden Daten beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, dann ist er auf sie, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen.

§ 10 Datenübermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stellen ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis (§ 45 Satz 2 Nr. 1, Satz 3) und sind sie der übermittelnden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist für die Zulässigkeit der Übermittlung ferner erforderlich, daß der Empfänger die Daten zur Erfüllung des gleichen Zweckes benötigt, zu dem sie die übermittelnde Stelle erhalten hat.

Entwurf HDSG

BDSG

(2) Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender Anwendung der Vorschriften über die Datenübermittlung an Behörden und sonstige öffentliche Stellen zulässig, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

§ 9 Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an andere als die in § 2 Abs. 1 genannten Stellen ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgabe erforderlich ist.

(2) Sie ist ferner zulässig, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten und die Einwilligung des Betroffenen nachweist; § 7 Abs. 3 gilt entsprechend. Auf den Nachweis der Einwilligung kann nur verzichtet werden, wenn keine Übermittlungssperre besteht und die Übermittlung wegen der Art der Daten, ihre Offenkundigkeit, wegen des Verwendungszweckes oder aus ähnlichen Gründen schutzwürdige Belange des Betroffenen nicht beeinträchtigt.

(3) Der Betroffene kann verlangen, daß die Übermittlung nach Abs. 2 gesperrt wird.

(4) Für personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden ist, gilt § 8 Abs. 2 entsprechend.

(5) Für die Übermittlung an Behörden oder sonstige Stellen außerhalb des Geltungsbereichs des Grundgesetzes sowie an über- und zwischenstaatliche Stellen finden die Absätze 1 bis 4 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen Anwendung.

§ 11 Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs

Die Übermittlung personenbezogener Daten an Personen und an andere Stellen als die in § 10 bezeichneten ist zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist oder soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis (§ 45 Satz 2 Nr. 1, Satz 3) und sind sie der übermittelnden Stelle von der zur Verschwiegenheit verpflichtenden Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist für die Zulässigkeit der Übermittlung ferner erforderlich, daß die gleichen Voraussetzungen gegeben sind, unter denen sie die zur Verschwiegenheit verpflichtete Person übermitteln dürfte. Für die Übermittlung an Behörden und sonstige Stellen außerhalb des Geltungsbereichs dieses Gesetzes sowie an über- und zwischenstaatliche Stellen finden die Sätze 1 und 2 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen Anwendung.

§ 10 Informationssysteme für statistische, planerische oder ähnliche Zwecke

(1) Für den Aufbau von Informationssystemen für statistische, planerische oder ähnliche Zwecke der in § 2 genannten Stellen können personenbezogene Daten übermittelt werden.

(2) Die nach Abs. 1 übermittelten personenbezogenen Daten dürfen nicht abgerufen, weiter übermittelt oder für andere als die in Abs. 1 genannten Zwecke genutzt werden.

(3) Die Verpflichtung nach Abs. 2 gilt auch für personenbezogene Daten, die beim Betroffenen für statistische, planerische oder ähnliche Zwecke erhoben worden sind.

Entsprechende Regelung fehlt.

Entwurf HDSG

§ 11 Verfahren für Auskünfte an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft über die zu seiner Person gespeicherten Daten zu erteilen.

(2) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
3. die Daten oder die Tatsache ihrer Speicherung nach einem Gesetz geheimgehalten werden müssen,
4. die Auskunft sich auf die Übermittlung personenbezogener Daten an die in § 14 Abs. 3 Nr. 1 genannten Behörden bezieht.

(3) Die Auskunft ist kostenfrei. Eine kostendeckende Gebühr kann erhoben werden, wenn die personenbezogenen Daten, auf die sich das Auskunftsersuchen bezieht, vom Betroffenen unmittelbar erfragt worden waren oder wenn der Betroffene ihrer Verarbeitung ausdrücklich zugestimmt hatte. Die Kostenpflicht entfällt, wenn durch besondere Umstände die Annahme gerechtfertigt war, daß personenbezogene Daten unrichtig oder unzulässig gespeichert werden oder wenn die Auskunft zur Berichtigung oder Löschung gespeicherter personenbezogener Daten geführt hat.

(4) Die Landesregierung bestimmt durch Rechtsverordnung das Nähere, insbesondere Form und Verfahren der Auskunftserteilung.

§ 12 Verfahren bei der Berichtigung, Sperrung und Löschung von Daten

(1) Unrichtige personenbezogene Daten sind von Amts wegen oder auf Antrag des Betroffenen zu berichtigen.

(2) Personenbezogene Daten sind von Amts wegen zu sperren,

1. wenn ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt,
2. wenn ihre Kenntnis für die speichernde Stelle zur

BDSG

§ 13 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung nach pflichtgemäßen Ermessen.

(2) Absatz 1 gilt nicht in den Fällen des § 12 Abs. 2 Nr. 1 und 2.

(3) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die rechtmäßige Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen einer dritten Person, geheimgehalten werden müssen,
4. die Auskunft sich auf die Übermittlung personenbezogener Daten an die in § 12 Abs. 2 Nr. 1 genannten Behörden bezieht.

(4) Die Auskunftserteilung ist gebührenpflichtig. Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die gebührenpflichtigen Tatbestände und die Höhe der Gebühr näher zu bestimmen sowie Ausnahmen von der Gebührenpflicht zuzulassen. Die Gebühren dürfen nur zur Deckung des unmittelbar auf Amtshandlungen dieser Art entfallenden Verwaltungsaufwandes erhoben werden. Ausnahmen von der Gebührenpflicht sind insbesondere in den Fällen zuzulassen, in denen durch besondere Umstände die Annahme gerechtfertigt wird, daß personenbezogene Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft zur Berichtigung oder Löschung gespeicherter personenbezogener Daten geführt hat. Im übrigen findet das Verwaltungskostengesetz Anwendung.

§ 14 Berichtigung, Sperrung und Löschung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu sperren, wenn ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt. Sie sind ferner zu sperren, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr verarbeitet,

Entwurf HDSG

rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht erforderlich ist.

Gesperrte Daten sind als solche zu kennzeichnen. Sie dürfen nicht mehr verarbeitet oder sonst genutzt werden, es sei denn, daß in den Fällen der Nr. 2 die Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist oder der Betroffene der Nutzung zugestimmt hat.

(3) Personenbezogene Daten sollen gelöscht werden, wenn ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Sie sind zu löschen, wenn ihre Speicherung unzulässig ist oder wenn es in den Fällen des Abs. 2 Nr. 2 der Betroffene beantragt.

§ 13 Verarbeitung im Auftrag

Verarbeiten in § 2 Abs. 1 genannte Stellen personenbezogene Daten im Auftrag andere Behörden, Stellen oder Personen, ist die Verarbeitung dieser Daten nur auf Weisung des Auftraggebers gestattet.

§ 14 Mitteilungs- und Veröffentlichungspflichten

(1) Die in § 2 Abs. 1 genannten Stellen teilen dem Datenschutzbeauftragten unverzüglich nach der ersten Einspeicherung

1. die Art der von ihnen oder in ihrem Auftrag gespeicherten Daten,
2. die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,
3. den betroffenen Personenkreis,
4. die Stellen, an die die Daten regelmäßig übermittelt werden und
5. die Art der übermittelten Daten

und fortlaufend die späteren Veränderungen mit. Zur Aufnahme in das Dateienregister können die in Abs. 3 Nr. 1 genannten Behörden und Stellen gesonderte Mitteilungen machen, die sich auf eine Übersicht über Art und Verwendungszweck der gespeicherten personenbezogenen Daten beschränken.

(2) Ferner sind die in Abs. 1 genannten Angaben nach der ersten Speicherung unverzüglich in einem amtlichen, von der Landesregierung zu bestimmenden Veröffentlichungsblatt bekanntzumachen; dabei ist auf das Dateienregister des Datenschutzbeauftragten hinzuweisen.

BDSG

insbesondere übermittelt, oder sonst genutzt werden, es sei denn, daß die Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist oder der Betroffene in die Nutzung eingewilligt hat.

(3) Personenbezogene Daten können gelöscht werden, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Sie sind zu löschen, wenn ihre Speicherung unzulässig war oder wenn es in den Fällen des Absatzes 2 Satz 2 der Betroffene verlangt.

§ 8 Verarbeitung personenbezogener Daten im Auftrag

(2) Die Vorschriften dieses Abschnittes gelten mit Ausnahme der §§ 15 bis 21 nicht für die in § 7 Abs. 1 und 2 genannten Stellen, soweit sie personenbezogene Daten im Auftrag verarbeiten. In diesen Fällen ist die Verarbeitung personenbezogener Daten in jeder ihrer in § 1 Abs. 1 genannten Phasen nur im Rahmen der Weisungen des Auftraggebers zulässig.

§ 19 Aufgaben des Bundesbeauftragten für den Datenschutz

(4) Der Bundesbeauftragte führt ein Register der automatisch betriebenen Dateien, in denen personenbezogene Daten gespeichert werden. Das Register kann von jedem eingesehen werden. Die in Absatz 1 Satz 1 genannten Behörden und sonstigen Stellen sind verpflichtet, die von ihnen automatisch betriebenen Dateien beim Bundesbeauftragten anzumelden. Das Bundesamt für Verfassungsschutz, der Bundesnachrichtendienst und der militärische Abschirmdienst sind von der Meldepflicht ausgenommen. Zu den Dateien der übrigen in § 12 Abs. 2 Nr. 1 genannten Bundesbehörden wird ein besonderes Register geführt. Es beschränkt sich auf eine Übersicht über Art und Verwendungszweck. Satz 2 findet auf dieses Register keine Anwendung. Das Nähere regelt der Bundesminister des Innern durch Rechtsverordnung.

§ 12 Veröffentlichung über die gespeicherten Daten

(1) Behörden und sonstige öffentliche Stellen geben

1. die Art der von ihnen oder in ihrem Auftrag gespeicherten personenbezogenen Daten,

Entwurf HDSG

(3) Abs. 2 gilt nicht

1. für das Landesamt für Verfassungsschutz, die Behörden der Staatsanwaltschaft und der Polizei sowie für Landesfinanzbehörden, soweit sie personenbezogene Daten zur Überwachung und Prüfung im Anwendungsbereich der Abgabenordnung in Dateien speichern,
2. für gesetzlich vorgeschriebene Register oder sonstige aufgrund von Rechtsvorschriften zu führende öffentliche Dateien.

§ 15 Technische und organisatorische Maßnahmen der Datensicherung

(1) Die in § 2 Abs. 1 genannten Stellen, die für eigene Aufgaben oder im Auftrag anderer Stellen personenbezogene Daten verarbeiten, haben die für den Datenschutz erforderlichen technischen, organisatorischen und perso-

BDSG

2. die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,
3. den betroffenen Personenkreis,
4. die Stellen, an die sie personenbezogene Daten regelmäßig übermitteln sowie
5. die Art der zu übermittelnden Daten

unverzüglich nach der ersten Einspeicherung in dem für ihren Bereich bestehenden Veröffentlichungsblatt für amtliche Bekanntmachungen bekannt. Auf Antrag sind dem Betroffenen die bisherigen Bekanntmachungen zugänglich zu machen.

(2) Absatz 1 gilt nicht

1. für die Behörden für Verfassungsschutz, den Bundesnachrichtendienst, den militärischen Abschirmdienst sowie andere Behörden des Bundesministers der Verteidigung, soweit die Sicherheit des Bundes berührt wird, das Bundeskriminalamt, die Behörden der Staatsanwaltschaft und der Polizei sowie für Bundes- und Landesfinanzbehörden, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung in Dateien speichern,
2. für die personenbezogenen Daten, die deshalb nach § 14 Abs. 2 Satz 2 gesperrt sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht nach § 14 Abs. 3 Satz 1 gelöscht werden dürfen,
3. für gesetzlich vorgeschriebene Register oder sonstige auf Grund von Rechts- oder veröffentlichten Verwaltungsvorschriften zu führende Dateien, soweit die Art der in ihnen gespeicherten personenbezogenen Daten, die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, der betroffene Personenkreis, die Stellen, an die personenbezogene Daten regelmäßig übermittelt werden, sowie die Art der zu übermittelnden Daten in Rechts- oder veröffentlichten Verwaltungsvorschriften festgelegt sind.

(3) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, für die in § 7 Abs. 1 Satz 1 genannten Behörden und sonstigen öffentlichen Stellen das Veröffentlichungsblatt sowie das Verfahren der Veröffentlichung zu bestimmen. Die Landesregierungen werden ermächtigt, durch Rechtsverordnungen für die in § 7 Abs. 2 Satz 1 genannten Behörden und sonstigen Stellen das Veröffentlichungsblatt sowie das Verfahren der Veröffentlichung zu bestimmen.

§ 6 Technische und organisatorische Maßnahmen

(1) Wer im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Personen oder Stellen personenbezogene Daten verarbeitet, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbeson-

Entwurf HDSG

nellen Maßnahmen zu treffen und bei automatischer Datenverarbeitung insbesondere die in der Anlage aufgeführten Anforderungen zu gewährleisten.

(2) Die Landesregierung wird ermächtigt, durch Rechtsverordnung die in der Anlage genannten Anforderungen nach dem jeweiligen Stand der Technik und Organisation fortzuschreiben.

§ 16 Datenverarbeitung in Wettbewerbsunternehmen

(1) Unbeschadet des § 2 Abs. 1 Satz 2 gelten für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen,

1. wenn sie personenbezogene Daten als Hilfsmittel für die Erfüllung ihrer Geschäftszwecke oder Ziele verarbeiten, §§ 22 bis 27 und § 30 des Bundesdatenschutzgesetzes oder,
2. wenn sie personenbezogene Daten für fremde Zwecke verarbeiten, nach Maßgabe des § 31 Abs. 1 Satz 1 die §§ 32 bis 37 und §§ 39, 40 des Bundesdatenschutzgesetzes

entsprechend.

(2) Die Landesregierung bestimmt durch Rechtsverordnung die nach §§ 30, 39 des Bundesdatenschutzgesetzes zuständige Aufsichtsbehörde.

§ 17 Datenverarbeitung für wissenschaftliche Zwecke

(1) Hochschulen und andere öffentliche Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher For-

BDSG

dere die in der Anlage zu diesem Gesetz genannten Anforderungen zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates die in der Anlage genannten Anforderungen nach dem jeweiligen Stand der Technik und Organisation fortzuschreiben. Stand der Technik und Organisation im Sinne dieses Gesetzes ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zur Gewährleistung der Durchführung dieses Gesetzes gesichert erscheinen läßt. Bei der Bestimmung des Standes der Technik und Organisation sind insbesondere vergleichbare Verfahren, Einrichtungen oder Betriebsweisen heranzuziehen, die mit Erfolg im Betrieb erprobt worden sind.

§ 22 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie geschützte personenbezogene Daten als Hilfsmittel für die Erfüllung ihrer Geschäftszwecke oder Ziele verarbeiten. Sie gelten mit Ausnahme der §§ 28 bis 30 nach Maßgabe von Satz 1 auch für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, soweit sie die Voraussetzungen von § 7 Abs. 1 Satz 1 oder § 7 Abs. 2 Satz 1 Nr. 1 erfüllen.

§ 31 Anwendungsbereich

(1) Für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts sowie für öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, soweit sie die Voraussetzungen von § 7 Abs. 1 Satz 1 oder § 7 Abs. 2 Satz 1 Nr. 1 erfüllen, gelten

1. die §§ 32 bis 35, soweit diese Stellen geschäftsmäßig geschützte personenbezogene Daten zum Zweck der Übermittlung speichern und übermitteln; dabei ist es unerheblich, ob die Daten vor der Übermittlung verändert werden,
2. § 36, soweit diese Stellen geschäftsmäßig geschützte personenbezogene Daten zum Zweck der Veränderung speichern, sie derart verändern, daß diese Daten sich weder auf eine bestimmte Person beziehen noch eine solche erkennen lassen (anonymisieren), und sie in dieser Form übermitteln,
3. § 37, soweit diese Stellen geschäftsmäßig geschützte personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten.

Entsprechende Regelung fehlt.

Entwurf HDSG	BDSG
schung können für bestimmte Forschungsvorhaben personenbezogene Daten speichern und verändern; hierfür können ihnen die in § 2 Abs. 1 genannten Behörden und öffentlichen Stellen personenbezogene Daten übermitteln. Die Datenverarbeitung nach Satz 1 ist nur zulässig, wenn die Betroffenen eingewilligt haben oder wenn ihre schutzwürdigen Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden.	
(2) Die nach Abs. 1 gespeicherten, veränderten und übermittelten und die nach Abs. 2 übermittelten personenbezogenen Daten dürfen nur mit Einwilligung der Betroffenen weiter übermittelt werden.	
(3) § 7 Abs. 2 und 3 ist entsprechend anzuwenden. § 14 gilt nicht.	
Dritter Abschnitt **Vorschriften zur Wahrung des Informationsgleichgewichts**	
§ 18 Informationsrechte des Landtags und der kommunalen Vertretungsorgane	Entsprechende Regelung fehlt.
(1) Die Hessische Zentrale für Datenverarbeitung, die Kommunalen Gebietsrechenzentren und die Landesbehörden, die Datenverarbeitungsanlagen betreiben, sind verpflichtet, dem Landtag, dem Präsidenten des Landtags und den Fraktionen des Landtags die von diesen im Rahmen ihrer Zuständigkeit verlangten Auskünfte aufgrund der gespeicherten Daten zu geben.	
(2) Die gleiche Auskunftspflicht obliegt der Hessischen Zentrale für Datenverarbeitung, dem zuständigen Kommunalen Gebietsrechenzentrum sowie den Gemeinden, Gemeindeverbänden und ihren Vereinigungen, wenn sie Datenverarbeitungsanlagen betreiben, gegenüber den Gemeindevertretungen, den Kreistagen und deren Fraktionen. Das Auskunftsverlangen der Fraktionen ist über den Gemeindevorstand bzw. den Kreisausschuß zu leiten.	
(3) Die Auskunft darf keine Daten einer bestimmten oder aus der Auskunft bestimmbaren Person enthalten. Sie ist abzulehnen, soweit sie die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.	
§ 19 Untersuchungen durch den Datenschutzbeauftragten	Entsprechende Regelung fehlt.
Der Landtag, der Präsident des Landtags, die Fraktionen des Landtags und die in § 18 Abs. 2 genannten Vertretungsorgane können verlangen, daß der Datenschutzbeauftragte untersucht, aus welchen Gründen Auskunftsersuchen nach § 18 nicht oder nicht ausreichend beantwortet worden sind.	

Entwurf HDSG

Vierter Abschnitt
Datenschutzbeauftragter

§ 20 Rechtsstellung

(1) Der Landtag wählt für die Dauer seiner Wahlperiode auf Vorschlag der Landesregierung einen Datenschutzbeauftragten. Der Datenschutzbeauftragte bleibt nach dem Ende der Wahlperiode bis zur Wahl seines Nachfolgers im Amt. Die Wiederwahl ist zulässig.

(2) Der Landtagspräsident verpflichtet den Datenschutzbeauftragten vor dem Landtag, sein Amt gerecht zu verwalten und die Verfassung des Landes Hessen und das Grundgesetz für die Bundesrepublik Deutschland getreulich zu wahren.

(3) Der Datenschutzbeauftragte steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis.

(4) Der Datenschutzbeauftragte ist auch nach Beendigung seines Amtsverhältnisses verpflichtet, über die ihm bei seiner amtlichen Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

§ 21 Unabhängigkeit

(1) Der Datenschutzbeauftragte ist in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen.

(2) Er kann jederzeit von seinem Amt zurücktreten. Der Landtag kann ihn seines Amtes entheben, wenn Tatsachen vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen.

§ 22 Aufgaben

(1) Der Datenschutzbeauftragte überwacht die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz bei den in § 2 Abs. 1 genannten Stellen sowie — soweit dies in Verträgen mit den genannten Behörden und Stellen vorgesehen ist — auch bei sonstigen Personen oder Personenvereinigungen.

(2) Der Datenschutzbeauftragte berät die Landesregierung und ihre Mitglieder sowie die übrigen in § 2 Abs. 1 genannten Stellen. Er unterrichtet die zuständige Aufsichtsbehörde über festgestellte Verstöße und gibt Anregungen zur Verbesserung des Datenschutzes.

(3) Der Datenschutzbeauftragte beobachtet die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der in § 2 Abs. 1 genannten Stellen dahingehend, ob sie das verfassungsmäßige Gefüge der Verfassungsorgane des Landes und der Organe der kommunalen Selbstverwaltung untereinander und zueinander verändern. Er soll Maßnahmen anregen, die ihm geeignet erscheinen, derartige Auswirkungen zu verhindern.

BDSG

Die Einrichtung des Bundesbeauftragten für den Datenschutz ist nicht vergleichbar.

Entwurf HDSG

§ 23 Dateienregister

(1) Der Datenschutzbeauftragte führt aufgrund der Mitteilungen nach § 14 Abs. 1 ein Register der automatisch betriebenen Dateien.

(2) Jeder kann in das Register Einsicht nehmen oder vom Datenschutzbeauftragten Auskunft darüber verlangen, gegenüber welcher Behörde oder öffentlichen Stelle er sein Recht nach § 5 geltend machen müßte. Auskunft und Einsicht sind kostenfrei.

§ 24 Anrufung des Datenschutzbeauftragten

Jeder kann sich an den Datenschutzbeauftragten wenden, wenn er annimmt, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt oder gefährdet zu sein. Auf Verlangen sind seine Angaben vertraulich zu behandeln.

§ 25 Auskunftsrecht des Datenschutzbeauftragten

Die in § 2 Abs. 1 genannten Stellen sind verpflichtet, den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist insbesondere

1. Auskunft zu geben,
2. Einsicht in Datenverarbeitungsprogramme und Programmdokumentationen sowie
3. Zutritt zu den Diensträumen zu gewähren.

§ 26 Zusammenarbeit mit anderen Stellen

Der Datenschutzbeauftragte soll mit den für die Überwachung des Datenschutzes im öffentlichen und im nicht-öffentlichen Bereich zuständigen Behörden und Stellen des Landes, der anderen Länder und des Bundes Verbindung halten und darauf hinwirken, daß die Aufgabe des Datenschutzes nach einheitlichen Grundsätzen verwirklicht wird. Er kann hierfür von den für die Überprüfung des Datenschutzes im nicht-öffentlichen Bereich zuständigen Behörden und öffentlichen Stellen die ihm erforderlich erscheinenden Auskünfte verlangen.

§ 27 Jahresbericht

(1) Bis zum 31. März jeden Jahres legt der Datenschutzbeauftragte dem Landtag und dem Ministerpräsidenten einen Bericht über das Ergebnis seiner Tätigkeit vor.

(2) Der Ministerpräsident führt eine Stellungnahme der Landesregierung zu dem Bericht herbei und legt diese dem Landtag vor.

(3) Zwischenberichte sind zulässig. Sie sind nach Abs. 2 zu behandeln.

§ 28 Vergütung, Personal- und Sachausstattung

(1) Die Vergütung des Datenschutzbeauftragten wird durch Vertrag mit der Landesregierung geregelt.

(2) Die Staatskanzlei stellt dem Datenschutzbeauftragten die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung.

BDSG

Entwurf HDSG

(3) Die dem Datenschutzbeauftragten zugewiesenen Bediensteten unterstehen insoweit seinen Weisungen.

(4) Für bestimmte Einzelfragen kann der Datenschutzbeauftragte auch Dritte zur Mitarbeit heranziehen, hierfür werden besondere Mittel zur Verfügung gestellt.

Fünfter Abschnitt
Schlußvorschriften

§ 29 Straftaten

(1) Wer unbefugt personenbezogene Daten

1. speichert,
2. verändert,
3. übermittelt,
4. abruft,
5. sich aus Dateien, die in Behältnissen verschlossen sind, verschafft oder
6. gesperrte Daten verwendet

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Handelt der Täter gegen Entgeld oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(3) Abs. 1 und 2 finden nur Anwendung, soweit die Tat nicht in anderen Vorschriften mit Strafe bedroht ist.

(4) Die Tat wird nur auf Antrag verfolgt.

§ 30 Übergangsvorschriften

Für personenbezogene Daten, die beim Inkrafttreten des Gesetzes gespeichert sind, gilt die Verpflichtung nach § 14 Abs. 2 mit der Maßgabe, daß die Veröffentlichunng binnen eines Jahres nach Inkrafttreten des Gesetzes auszuführen ist.

§ 31 Fortgeltende Vorschriften

Besondere Vorschriften zum Datenschutz in anderen Gesetzen des Landes gehen den Vorschriften dieses Gesetzes vor.

§ 32 Aufhebung bisherigen Rechts

Das Datenschutzgesetz vom 7. Oktober 1970 (GVBl. I S. 625), geändert durch das Gesetz vom 4. September 1974 (GVBl. I S. 361), wird aufgehoben.

§ 33 Inkrafttreten

Dieses Gesetz tritt einen Monat nach Verkündung in Kraft. Abweichend davon treten § 11 Abs. 4, § 14, § 15 Abs. 2, § 23 und § 30 am Tage nach der Verkündung des Gesetzes in Kraft.

BDSG

§ 41 Straftaten

(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,

1. übermittelt oder verändert oder
2. abruft oder sich aus in Behältnissen verschlossenen Dateien verschafft,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Handelt der Täter gegen Entgeld oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(3) Die Tat wird nur auf Antrag verfolgt.

§ 47 Inkrafttreten

Dieses Gesetz tritt am 1. Januar 1978 in Kraft. Abweichend davon treten in Kraft:

1. § 12 Abs. 3, § 13 Abs. 4, §§ 16 und 19 Abs. 4 Satz 8 am Tage nach der Verkündung des Gesetzes,
2. §§ 17, 18, 28 und 38 am 1. Juli 1977,
3. § 6 und die Anlage zu § 6 Abs. 1 Satz 1 am 1. Januar 1979.

Entwurf HDSG

Anlage zu § 15 E

Werden personenbezogene Daten automatisch verarbeitet, sind zur Ausführung der Vorschriften dieses Gesetzes Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

1. Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),
2. Personen, die bei der Verarbeitung personenbezogener Daten tätig sind, daran zu hindern, daß sie Datenträger unbefugt entfernen (Abgangskontrolle),
3. die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),
4. die Benutzung von Datenverarbeitungssystemen, aus denen oder in die personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden, durch unbefugte Personen zu verhindern (Benutzungskontrolle),
5. zu gewährleisten, daß die zur Benutzung eines Datenverarbeitungssystems Berechtigten durch selbsttätige Einrichtungen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),
6. zu gewährleisten, daß überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden können (Übermittlungskontrolle),
7. zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),
8. zu gewährleisten, daß personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
9. zu gewährleisten, daß bei der Übermittlung personenbezogener Daten sowie beim Transport entsprechender Datenträger diese nicht unbefugt gelesen, verändert oder gelöscht werden können (Transportkontrolle),
10. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

BDSG

Anlage zu § 6 Abs. 1 S. 1

gleichlautend

SACHWÖRTERVERZEICHNIS

(I, II, III, IV, V und VI bezeichnen den Ersten, Zweiten, Dritten, Vierten, Fünften bzw. Sechsten Tätigkeitsbericht, die arabischen Ziffern die Abschnitte der Berichte; 1. Z bezeichnet den Zwischenbericht vom 6. 2. 1976; s. bedeutet: siehe; s. a. bedeutet: siehe auch)