72 der Beilagen zu den stenographischen Protokollen des Nationalrates XIV. GP

1975 12 17

Regierungsvorlage

Bundesgesetz vom XXXXXXXXXX über den Schutz personsbezogener Daten (Datenschutzgesetz — DSG)

Der Nationalrat hat beschlossen:

I. ALLGEMEINE BESTIMMUNGEN

Zuständigkeit

§ 1. (Verfassungsbestimmung) Bundessache ist die Gesetzgebung hinsichtlich des Schutzes personsbezogener Daten, die mit Hilfe der elektronischen Datenverarbeitung oder vergleichbarer technischer Hilfsmittel verarbeitet werden. Die Vollziehung solcher Bundesgesetze steht dem Bund zu, soweit die Daten weder von oder im Auftrage eines Landes bzw. von oder im Auftrage von juristischen Personen, die durch Gesetz eingerichtet sind, und deren Einrichtung in der Vollziehung in die Zuständigkeit der Länder fällt, verarbeitet werden. Die die Ermittlung und Verarbeitung von Daten regelnden Bundesgesetze können vorsehen, daß die Durchführungsverordnungen zu den nach dem ersten Satz ergehenden Bundesgesetzen auch in den Fällen, in denen sonst die Vollziehung den Ländern zusteht, vom Bund zu erlassen sind.

Begriffsbestimmungen

§ 2. Im Sinne dieses Bundesgesetzes bedeuten:

1. personsbezogene Daten: Angaben, die Aussagen über eine bestimmte oder mit Wahrscheinlichkeit bestimmbare natürliche oder juristische Person oder handelsrechtliche Personengesellschaft enthalten einschließlich von Personenkennzeichen;

2. Betroffene: Personen oder handelsrechtliche Personengesellschaften, über die Daten nach Z. 1 erhoben oder verarbeitet werden;

3. Datenverarbeitung oder Verarbeitung von Daten: das Speichern, Verändern, Verknüpfen, Weitergeben oder Löschen von personsbezogenen Daten ohne Rücksicht auf die dabei angewendeten Verfahren;

4. Erhebung oder Erheben: das Ermitteln personsbezogener Daten unter mündlicher oder schriftlicher Mitwirkung des Betroffenen;

5. Speicherung oder Speichern: das Festhalten von Daten auf einem Datenträger;

6. Veränderung oder Verändern: das inhaltliche Umgestalten gespeicherter Daten;

7. Verknüpfung oder Verknüpfen: das einmalige oder dauernde Zusammenfassen von für verschiedene Datenbanken erhobenen oder in verschiedenen Datenbanken gespeicherten personsbezogenen Daten in einer einzigen Datenbank;

8. Weitergabe oder Weitergeben: das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an Personen oder Stellen außerhalb der Einrichtung, bei der oder in deren Auftrag die Daten verarbeitet werden;

9. Löschung oder Löschen: das Unkenntlichmachen von gespeicherten Daten ohne die Möglichkeit ihrer Rekonstruierung;

10. Datenbank: eine nach bestimmten Merkmalen geordnete Sammlung personsbezogener Daten, die mit Hilfe der elektronischen Datenverarbeitung oder vergleichbarer technischer Hilfsmittel (automatisierte Datenverarbeitung) nach anderen Merkmalen umgeordnet oder verarbeitet werden können, einschließlich der Datenträger und der maschinellen Einrichtungen.

Anwendung im Bereich der Vollziehung des Bundes

§ 3. (1) Die Bestimmungen der Abschnitte I bis IV, VI und VII sind auf die Erhebung und Verarbeitung personsbezogener Daten durch oder im Auftrage von Rechtsträgern anzuwenden, die unmittelbar durch Gesetz errichtet sind, soweit es sich nicht um Rechtsträger nach § 4 handelt.

(2) Dieses Bundesgesetz ist mit Ausnahme der Bestimmungen des § 27 und des § 29 auf Daten-

banken, die von oder im Auftrage von Organen der Gesetzgebung geführt werden, nicht anzuwenden.

(3) Auf die Oesterreichische Nationalbank und auf die Österreichische Postsparkasse sind die Abschnitte II bis IV dieses Bundesgesetzes nicht anzuwenden.

Anwendung im Bereich der Vollziehung der Länder

§ 4. Auf die Verarbeitung personsbezogener Daten in Datenbanken von oder im Auftrage von juristischen Personen, die durch Gesetze eingerichtet sind, und deren Einrichtung in der Vollziehung in die Zuständigkeit der Länder fällt, sowie von oder im Auftrage von Gemeinden oder Gemeindeverbänden sind die Bestimmungen der Abschnitte I bis IV, VI und VII dieses Bundesgesetzes mit der Maßnahme anzuwenden,

1. daß die Datenbank-Verordnung (§ 9) und die Höhe der Verwaltungsabgabe für die Erteilung einer Auskunft (§ 10 Abs. 3) durch die Landesregierung festzulegen sind;

2. daß die Pflicht zur Mitteilung gemäß § 13 Abs. 1 gegenüber der Landesregierung besteht;

3. daß diese Datenbanken in ein von der Landesregierung in einem Kundmachungsblatt des Landes zu verlautbarendes Datenbanken-Verzeichnis des Landes aufzunehmen sind;

4. daß für jedes Land beim Amt der Landesregierung eine Landes-Datenschutzkommission einzurichten ist, deren Mitglieder zum Landtag wählbar sein müssen und von der Landesregierung bestellt werden, die der Landesregierung jährlich über ihre Tätigkeit zu berichten hat und deren Bericht von der Landesregierung dem Landtag zur Kenntnis zu bringen ist;

5. daß Mitglieder der Bundes-Datenschutzkommission nicht zu Mitgliedern einer Landes-Datenschutzkommission bestellt werden dürfen;

6. daß die Landes-Datenschutzkommission zur Entscheidung über Beschwerden gemäß § 20 zuständig ist;

7. daß die Entschädigung für die Mitglieder der Landes-Datenschutzkommission (§ 18) jährlich durch Verordnung der Landesregierung festzusetzen ist;

8. daß zu besetzende Stellen in der Landes-Datenschutzkommission von der Landesregierung zur allgemeinen Bewerbung in der für allgemeine Kundmachungen des Landes bestimmten Landeszeitung auszuschreiben sind.

Öffentlich zugängliche Datenbanken

§ 5. Auf Datenbanken, die auf Grund gesetzlicher Bestimmungen öffentlich zugänglich sind, ist dieses Bundesgesetz nicht anzuwenden.

II. VERARBEITUNG PERSONSBEZOGENER DATEN

Zulässigkeit der Erhebung und Verarbeitung

§ 6. Personsbezogene Daten dürfen zum Zwecke ihrer Verwendung in Datenbanken nur erhoben und verarbeitet werden, wenn dafür eine ausdrückliche gesetzliche Ermächtigung besteht oder soweit dies für den Rechtsträger zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bildet.

Weitergabe von Daten

§ 7. (1) Personsbezogene Daten dürfen, soweit sie der Amtsverschwiegenheit (Art. 20 Abs. 3 B-VG) oder einer gesetzlich festgelegten beruflichen Verschwiegenheitspflicht unterliegen, in keiner wie immer gearteten Weise aus einer Datenbank weitergegeben werden.

(2) Die Bestimmung des Abs. 1 ist nicht anzuwenden, wenn

1. gesetzlich etwas anderes bestimmt ist oder

2. der Betroffene der Weitergabe schriftlich zugestimmt hat oder

3. durch geeignete Maßnahmen sichergestellt wird, daß der Betroffene nicht bestimmbar ist, soweit es sich dabei um personsbezogene Daten handelt, deren Geheimhaltung ausschließlich im Interesse des Betroffenen geboten ist.

(3) Eine Weitergabe an Organe des Bundes, der Länder, der Gemeinden und der gesetzlichen beruflichen Vertretungen ist weiters insoweit zulässig, als die Daten für den Empfänger zur Wahrnehmung der ihm gesetzlich übertragenen Aufgabe eine wesentliche Voraussetzung bilden.

Verknüpfung von Daten

§ 8. Personsbezogene Daten, die in einer Datenbank gespeichert werden, dürfen mit in anderen Datenbanken gespeicherten personsbezogenen Daten nur insoweit verknüpft werden, als dies gesetzlich ausdrücklich vorgesehen oder mit dem Zweck, für den die Daten ermittelt wurden, vereinbar ist.

Datenbank-Verordnung

§ 9. (1) Für jede Datenbank ist durch Verordnung des Bundesministers, dem die Aufsicht über die die Datenbank führende Einrichtung obliegt, nach Anhörung des Bundeskanzlers eine Datenbank-Verordnung zu erlassen, die unter Bedachtnahme auf die wirtschaftliche Vertretbarkeit und auf die technische Möglichkeit jene Maßnahmen organisatorischer, personeller, technischer und baulicher Art festzulegen hat, die je nach Art der personsbezogenen Daten und der technischen Ausstattung sowie des Umfanges der Datenbank notwendig sind, um sicherzustellen, daß personsbezogene Daten Dritten rechts-

widrig weder zur Kenntnis gelangen noch weitergegeben noch durch dazu nicht berechtigte Personen verändert, verknüpft oder gelöscht werden können.

(2) Die Datenbank-Verordnung hat insbesondere Bestimmungen zu enthalten über den Zugang zur Datenbank und zu den Datenträgern, über die vorzusehenden technischen und baulichen Sicherheitsvorkehrungen (physische Datensicherung), um eine unbefugte, fahrlässige oder zufällige Löschung oder Veränderung von Daten und Programmen zu verhindern, über die Durchführung von Prüfungen von Maschinen und Programmen mit personsbezogenen Daten, über die Protokollierung von Datenweitergaben und die Dauer der Aufbewahrung der Protokolle sowie über die zur Datenveränderung und Datenweitergabe berechtigten Personengruppen und deren Verpflichtung zur Geheimhaltung der ihnen im Zusammenhang mit der Datenverarbeitung bekanntgewordenen Tatsachen und Informationen.

(3) Sollen personsbezogene Daten unter der Voraussetzung des § 7 Abs. 2 Z. 3 weitergegeben werden, so hat die Datenbank-Verordnung Bestimmungen über die Sicherstellung der Anonymisierung dieser Daten zu enthalten.

(4) Weiters ist in der Datenbank-Verordnung unter Bedachtnahme auf § 7 die Aus- und Weitergabe personsbezogener Daten in einer Weise zu regeln, daß dadurch die berechtigten Interessen der Betroffenen an der Geheimhaltung personsbezogener Daten gewährleistet werden.

(5) Die Datenbank-Verordnung ist durch den zuständigen Bundesminister der jeweiligen technischen Entwicklung anzupassen, sofern es die im Abs. 1 und im Abs. 4 genannten Zwecke erfordern.

Auskunftsrecht

§ 10. (1) Dem Betroffenen sind auf schriftlichen Antrag bei der die Datenbank führenden Einrichtung personsbezogene Daten in allgemein verständlicher, lesbarer Form sowie die Rechtsgrundlage für deren Erhebung und Verarbeitung schriftlich binnen vier Wochen mitzuteilen, soweit es sich dabei nicht um solche Daten handelt, die auf Grund einer ausdrücklichen gesetzlichen Anordnung oder im Interesse einer Gebietskörperschaft auch ihm gegenüber geheimzuhalten sind.

(2) Wird einem Antrag nach Abs. 1 nicht vollinhaltlich stattgegeben, so ist dies dem Betroffenen schriftlich mitzuteilen.

(3) Für die Erteilung einer Auskunft kann von dem für die Erlassung der Datenbank-Verordnung zuständigen Bundesminister (§ 9) eine Verwaltungsabgabe vorgeschrieben werden, deren Höhe durch Verordnung unter Bedachtnahme auf die durchschnittlichen tatsächlichen Kosten einer Auskunftserteilung pauschaliert festzusetzen ist.

(4) Abs. 1 ist nicht anzuwenden, soweit die Daten dem Betroffenen von der die Datenbank führenden Einrichtung bereits mitgeteilt wurden.

Berichtigungspflicht

§ 11. (1) Jede Einrichtung, die den Auftrag zur Verarbeitung personsbezogener Daten in einer Datenbank gegeben hat, hat unrichtige, unvollständige oder entgegen der Bestimmung des § 6 erhobene oder verarbeitete personsbezogene Daten von Amts wegen, auf Grund einer Entscheidung der für die Feststellung der Daten sachlich zuständigen Behörde, auf Antrag des Betroffenen oder auf Grund einer Entscheidung der Bundes-Datenschutzkommission unverzüglich, längstens jedoch binnen zwei Wochen nach Klärung der der Datenverarbeitung zugrunde zu legenden Angaben zu berichtigen, zu löschen oder die Berichtigung oder Löschung zu veranlassen. Die Prüfung des Berichtigungsantrages hat unverzüglich zu erfolgen.

(2) Wird ein Antrag (Abs. 1) des Betroffenen abgelehnt, so ist ihm dies schriftlich mitzuteilen.

(3) Der Beweis der Richtigkeit der verarbeiteten personsbezogenen Daten obliegt der Einrichtung, die den Auftrag zur Verarbeitung gegeben hat, soweit die Daten nicht ausschließlich auf Grund von Angaben des Betroffenen erhoben wurden.

(4) Ist die Berichtigung oder Löschung auf Antrag des Betroffenen oder auf Grund einer Entscheidung der Bundes-Datenschutzkommission durchgeführt worden, so ist der Betroffene, im Falle der Berichtigung oder Löschung auf Grund einer Entscheidung der Bundes-Datenschutzkommission auch diese, von der Berichtigung oder Löschung zu verständigen. Die Benachrichtigung des Betroffenen hat zu entfallen, soweit ihm die Berichtigung oder Löschung von der für die Feststellung der Daten sachlich zuständigen Behörde bereits mitgeteilt wurde.

(5) Wurden im Sinne des Abs. 1 berichtigte oder gelöschte personsbezogene Daten vor der Berichtigung oder Löschung weitergegeben (§ 7) oder verbunden (§ 8), so hat die datenverarbeitende Einrichtung die Berichtigung oder Löschung dem Empfänger dieser Daten mitzuteilen, sofern der Betroffene es verlangt, ein berechtigtes Interesse glaubhaft macht und der Empfänger noch feststellbar ist.

(6) Eine Berichtigung und eine Löschung sind ausgeschlossen, wenn die personsbezogenen Daten im Zeitpunkt ihrer Ermittlung richtig und vollständig waren und der Zweck der Ermittlung oder der Verarbeitung der Daten eine

Veränderung der Daten in Entsprechung von Änderungen des ihnen zugrunde liegenden Sachverhaltes ausschließt.

(7) Erfolgt eine Berichtigung oder Löschung auf Grund einer Entscheidung der für die Feststellung der Daten sachlich zuständigen Behörde, so ist die Einrichtung, die den Auftrag zur Datenverarbeitung gegeben hat, an diese Entscheidung gebunden.

Ausnahme für das Strafregister

§ 12. Die Bestimmungen des § 10 und des § 11 dieses Bundesgesetzes sind auf das von der Bundespolizeidirektion Wien geführte Strafregister (Strafregistergesetz 1968, BGBl. Nr. 277, in der Fassung der Strafregisternovelle 1972, BGBl. Nr. 101, und der Strafregisternovelle 1974, BGBl. Nr. 797) nicht anzuwenden.

Kundmachung eines Verzeichnisses der Datenbanken

§ 13. (1) Jede Einrichtung, bei der oder in deren Auftrag (§ 14) eine Datenbank geführt wird, hat jährlich bis zum 1. Feber dem Bundeskanzleramt die Führung und die Rechtsgrundlage sowie den Zweck und die Verwendung der Datenbank, die Art der in dieser Datenbank verarbeiteten personsbezogenen Daten und den Kreis der Betroffenen schriftlich mitzuteilen.

(2) Das Bundeskanzleramt hat jeweils bis spätestens 10. Mai jedes Jahres ein Verzeichnis der Datenbank im Amtsblatt zur „Wiener Zeitung" zu verlautbaren. In der Verlautbarung sind auch die Art der in der betreffenden Datenbank gespeicherten personsbezogenen Daten, der Kreis der Betroffenen und der Zweck der Datenbank anzugeben.

III. VERTRAGLICHE INANSPRUCHNAHME VON DATENVERARBEITUNG DURCH DIE IN § 3 UND 4 GENANNTEN RECHTSTRÄGER

Voraussetzungen

§ 14. (1) Die in § 3 und in § 4 genannten Rechtsträger dürfen nur unter den Voraussetzungen des § 6 andere Rechtsträger oder sonstige Personen zur Verarbeitung personsbezogener Daten in Datenbanken in Anspruch nehmen.

(2) Im Falle der Inanspruchnahme anderer Rechtsträger oder sonstiger Personen zur Verarbeitung personsbezogener Daten haben die in § 3 und in § 4 genannten Rechtsträger vertraglich sicherzustellen, daß bei der Verarbeitung dieser Daten die Bestimmungen des Abschnittes II eingehalten werden. In Verträgen, mit denen andere Rechtsträger oder sonstige Personen mit der Verarbeitung personsbezogener Daten durch die in § 3 und 4 genannten Rechtsträger betraut werden, ist insbesondere eine den Anforderungen des § 9 entsprechende Datenbank-Betriebsordnung zu vereinbaren.

(3) Die Verarbeitung von personsbezogenen Daten auf Grund dieses Abschnittes ist in das Verzeichnis der Datenbanken (§ 13) einzubeziehen, soweit sie nicht bloß vorübergehend ist.

IV. BUNDES-DATENSCHUTZKOMMISSION

Einrichtung und Zusammensetzung

§ 15. (1) Zur Gewährleistung der Einhaltung der Bestimmungen der Abschnitte II und III wird beim Bundeskanzleramt die Bundes-Datenschutzkommission eingerichtet.

(2) Die Bundes-Datenschutzkommission besteht aus fünfzehn Mitgliedern, von denen acht Mitglieder dem Richterstand angehören müssen. Die übrigen Mitglieder müssen auf dem Gebiet des Datenschutzes besondere Erfahrungen aufweisen.

(3) Der Besetzung von Stellen in der Bundes-Datenschutzkommission hat eine Ausschreibung nach dem Ausschreibungsgesetz, BGBl. Nr. 700/1974, vorzugehen.

(4) Die Mitglieder der Bundes-Datenschutzkommission ernennt der Bundespräsident auf Vorschlag der Bundesregierung für die Dauer von sechs Jahren.

(5) Der Bundes-Datenschutzkommission können nicht angehören:

1. Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre;

2. Personen, die in einer Datenbank, auf die die Bestimmungen dieses Bundesgesetzes Anwendung finden, beschäftigt sind;

3. Mitglieder einer Landes-Datenschutzkommission;

4. Personen, die zum Nationalrat nicht wählbar sind.

(6) Hat ein Mitglied der Bundes-Datenschutzkommission drei aufeinanderfolgenden Einladungen zu einer Verhandlung ohne genügende Entschuldigung keine Folge geleistet oder tritt bei einem Mitglied ein Ausschließungsgrund des Abs. 5 nachträglich ein, so hat dies nach seiner Anhörung die Vollversammlung der Bundes-Datenschutzkommission festzustellen. Diese Feststellung hat den Verlust der Mitgliedschaft zur Folge. Im übrigen kann ein Mitglied der Bundes-Datenschutzkommission nur aus einem schwerwiegenden Grund durch Beschluß der Vollversammlung der Bundes-Datenschutzkommission, dem mindestens zwei Drittel ihrer Mitglieder zustimmen müssen, seines Amtes für verlustig erklärt werden.

(7) Scheidet ein Mitglied der Bundes-Datenschutzkommission wegen Todes, freiwillig oder gemäß Abs. 6 vorzeitig aus, so ist an seiner Stelle ein neues Mitglied zu ernennen (Abs. 4). Abs. 2 findet hiebei mit der Maßgabe Anwendung, daß an Stelle eines Richters wieder ein Richter und an Stelle eines anderen Mitgliedes nur wieder ein solches ernannt werden darf.

Unabhängigkeit und Weisungsfreiheit

§ 16. Die Mitglieder der Bundes-Datenschutzkommission sind in Ausübung ihres Amtes unabhängig und an keine Weisungen gebunden.

Vorsitzender

§ 17. Die Vollversammlung der Bundes-Datenschutzkommission wählt mit einfacher Mehrheit aus dem Kreis der richterlichen Mitglieder einen Vorsitzenden und einen stellvertretenden Vorsitzenden.

Entschädigung der Mitglieder

§ 18. Den Mitgliedern der Bundes-Datenschutzkommission gebührt eine Entschädigung, die von der Bundesregierung durch Verordnung unter Bedachtnahme auf die Bedeutung und den Umfang der von der Bundes-Datenschutzkommission zu besorgenden Aufgaben jährlich festzusetzen ist.

Senate und Verfahren

§ 19. (1) Zur Entscheidung über jede Beschwerde wird ein aus fünf Mitgliedern bestehender Senat gebildet. Drei Mitglieder des Senates werden aus dem Kreise der richterlichen Mitglieder der Bundes-Datenschutzkommission, zwei weitere aus dem Kreis der übrigen Mitglieder vor Beginn des Verfahrens durch das Los bestimmt. Für jedes Mitglied eines Senates ist nach dem gleichen Verfahren ein Ersatzmitglied zu bestellen, das im Falle der Verhinderung des Mitgliedes an dessen Stelle tritt.

(2) Den Vorsitz führt im Senat der Vorsitzende der Bundes-Datenschutzkommission, sofern er ihm angehört, ansonsten der stellvertretende Vorsitzende. Ist auch dieser nicht Mitglied des Senates, so ist der Vorsitzende des Senates vom Senat aus dem Kreis der richterlichen Mitglieder zu wählen.

(3) Der Senat entscheidet mit einfacher Stimmenmehrheit. Stimmenthaltung ist unzulässig. Der Vorsitzende gibt seine Stimme als letzter ab.

(4) Auf das Verfahren der Bundes-Datenschutzkommission ist im übrigen das AVG 1950 anzuwenden.

(5) Wenn die Bundes-Datenschutzkommission eine Verletzung von Bestimmungen dieses Bundesgesetzes oder der auf Grund dieses Bundesgesetzes erlassenen Verordnungen festgestellt hat, so sind die Verwaltungsbehörden verpflichtet, mit den ihnen zu Gebote stehenden rechtlichen Mitteln unverzüglich den der Rechtsanschauung der Bundes-Datenschutzkommission entsprechenden Rechtszustand herzustellen. In den Bescheiden der Bundes-Datenschutzkommission ist die Behörde zu bestimmen, die den Bescheid zu vollstrecken hat. Das Vollstreckungsverfahren richtet sich nach den für diese Behörde sonst geltenden Vorschriften.

Beschwerdeverfahren

§ 20. (1) Die Bundes-Datenschutzkommission erkennt, soweit nicht ein ordentliches Gericht zuständig oder der Antrag des Betroffenen auf Berichtigung oder Löschung (§ 11) bereits Gegenstand eines Verfahrens vor der sachlich zuständigen Behörde ist, in erster Instanz über Beschwerden wegen Verletzung von Bestimmungen dieses Bundesgesetzes oder der auf Grund dieses Bundesgesetzes erlassenen Verordnungen, soweit der Beschwerdeführer behauptet, dadurch in seinen Rechten verletzt worden zu sein, sowie über Anträge gemäß Abs. 3.

(2) Erfolgte eine Berichtigung oder Löschung auf Grund einer Entscheidung der für die Feststellung der Daten sachlich zuständigen Behörde (§ 11 Abs. 6), so ist die Bundes-Datenschutzkommission an die Entscheidung gebunden.

(3) Wird in einem Verwaltungsverfahren, in dem personsbezogene Daten aus einer den Bestimmungen dieses Bundesgesetzes unterliegenden Datenbank verwertet werden, die Verletzung von Bestimmungen dieses Bundesgesetzes oder der auf Grund dieses Bundesgesetzes erlassenen Verordnungen behauptet, so ist das Verwaltungsverfahren, außer bei Gefahr von Verzug, bis zur Entscheidung der Bundes-Datenschutzkommission auszusetzen (§ 38 AVG). Gleichzeitig ist ein solches Verfahren zu beantragen.

(4) Entscheidungen der Bundes-Datenschutzkommission unterliegen nicht der Aufhebung oder Abänderung im Verwaltungswege. Die Beschwerde an den Verwaltungsgerichtshof ist zulässig.

Amtswegige Einleitung eines Verfahrens

§ 21. (1) Ergibt sich während eines Verfahrens nach § 20 die Vermutung der Verletzung von Bestimmungen dieses Bundesgesetzes oder der auf Grund dieses Bundesgesetzes erlassenen Verordnungen auch für andere Betroffene, so hat die Bundes-Datenschutzkommission von Amts wegen unter Benachrichtigung der Betroffenen ein Verfahren zur Prüfung dieser Vermutungen einzuleiten, wobei den Betroffenen Parteistellung (§ 8 AVG) zukommt.

(2) Die Bestimmungen des § 19 und des § 20 Abs. 2 und 3 sind auch auf dieses Verfahren anzuwenden.

Verbindung eingeleiteter Verfahren

§ 22. Wenn die Zweckmäßigkeit, Raschheit, Einfachheit und Kostenersparnis von Verfahren es erfordern, hat die Vollversammlung der Bundes-Datenschutzkommission eingeleitete Verfahren (§ 20, § 21) zu verbinden und einem Senat zur Entscheidung zuzuweisen. Auf die Zusammensetzung dieses Senates ist § 19 anzuwenden.

Veröffentlichung der Entscheidungen und Bericht

§ 23. (1) Die Entscheidungen der Bundes-Datenschutzkommission sind zu veröffentlichen, soweit dadurch nicht berechtigte Interessen der Betroffenen verletzt werden.

(2) Die Bundes-Datenschutzkommission hat jährlich der Bundesregierung über ihre Tätigkeit zu berichten, wobei insbesondere auf beobachtete Erfahrungen bei der Durchführung von Verfahren nach diesem Bundesgesetz Bedacht zu nehmen ist. Dieser Bericht ist durch die Bundesregierung dem Nationalrat zur Kenntnis zu bringen.

V. PRIVATE DATENBANKEN

Beschränkung privater Datenbanken

§ 24. Die Ermittlung und Erhebung personsbezogener Daten und ihre Verarbeitung in einer nicht den Bestimmungen des § 3 oder des § 4 unterliegenden Datenbank eines Unternehmens (§ 2 des Umsatzsteuergesetzes 1972, BGBl. Nr. 223) oder eines Vereines haben in einer dem Zweck des Unternehmens oder Vereines entsprechenden Art sowie in einem das Privat- und Familienleben der Betroffenen achtenden Umfang zu erfolgen.

Heranziehung ausländischer Datenverarbeitungsanlagen

§ 25. Die Heranziehung von nicht innerhalb des österreichischen Bundesgebietes gelegenen Datenverarbeitungsanlagen zur Verarbeitung personsbezogener Daten durch einen nicht den Bestimmungen des § 3 und des § 4 unterliegenden Rechtsträger, der seinen Sitz in Österreich hat, darf nur unter Einhaltung der Bestimmungen des § 24 erfolgen.

Aufsicht

§ 26. Die Beobachtung und Durchsetzung der Einhaltung der Bestimmungen des § 24 und § 25 obliegt der Behörde, die für die allgemeine Aufsicht über den die Datenbank führenden Rechtsträger zuständig ist. Ist für den die Daten erhebenden oder verarbeitenden Rechtsträger nicht die Zuständigkeit einer solchen Behörde gegeben, so ist die Aufsicht von der örtlich zuständigen Bezirksverwaltungsbehörde (§ 3 AVG) wahrzunehmen.

(2) Die Aufsichtsbehörde (Abs. 1) kann neben den ihr auf Grund anderer Gesetze zustehenden Mitteln durch Bescheid die Einstellung oder Einschränkung einer den Bestimmungen des § 24 oder des § 25 nicht entsprechenden Ermittlung oder Verarbeitung von Daten verfügen.

VI. STRAFBESTIMMUNGEN

Datenmißbrauch

§ 27. Wer personsbezogene Daten, die ihm ausschließlich kraft seiner Beschäftigung mit Aufgaben der Datenverarbeitung anvertraut oder zugänglich geworden sind, entgegen den Bestimmungen des § 7 offenbart oder verwertet, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

Geheimnisbruch in privaten Datenbanken

§ 28. (1) Wer ein Geheimnis offenbart oder verwertet, das ihm bei berufsmäßiger Beschäftigung mit Aufgaben der Datenverarbeitung in einer Datenbank (§ 2 Z. 10) anderer als der in den § 3 und § 4 bezeichneten Art ausschließlich kraft seines Berufes anvertraut worden oder zugänglich geworden ist und dessen Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse der Person zu verletzen, auf die sich die Daten beziehen, ist vom Gericht mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nicht zu bestrafen, wenn die Offenbarung oder Verwertung nach Inhalt und Form durch ein öffentliches oder ein berechtigtes privates Interesse gerechtfertigt ist.

(3) Der Täter ist nur auf Verlangen des in seinem Interesse an der Geheimhaltung Verletzten (Abs. 1) zu verfolgen.

Unbefugte Verschaffung von Daten

§ 29. (1) Wer sich widerrechtlich personsbezogene Daten, deren Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse des Betroffenen (§ 2 Z. 2) zu verletzen, aus einer Datenbank mit dem Vorsatz verschafft, die Daten zu offenbaren oder zu verwerten, ist vom Gericht mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.

(2) Der Täter ist nur auf Verlangen des Betroffenen zu verfolgen. Wird die Tat jedoch in bezug auf eine Datenbank der in den §§ 3 und 4 bezeichneten Art begangen, so hat der öffentliche Ankläger den Täter mit Ermächtigung des Verletzten (Abs. 1) zu verfolgen.

VII. SCHLUSSBESTIMMUNGEN

Inkrafttreten

§ 30. (1) Dieses Bundesgesetz tritt mit 1. Jänner 1977 in Kraft.

(2) Verordnungen auf Grund der Bestimmungen dieses Bundesgesetzes können bereits von dem seiner Kundmachung folgenden Tag an erlassen werden. Diese Verordnungen dürfen frühestens mit dem in Abs. 1 bezeichneten Zeitpunkt in Kraft gesetzt werden.

(3) Für im Zeitpunkt des Inkrafttretens bereits eingerichtete Datenbanken ist die Datenbank-Verordnung bis spätestens 1. Jänner 1978 zu erlassen.

Eigener Wirkungsbereich der Gemeinde

§ 31. Soweit dieses Bundesgesetz auf Datenbanken anzuwenden ist, die von oder im Auftrage von Gemeinden geführt werden, sind von der Gemeinde nach diesem Bundesgesetz durchzuführende Aufgaben solche des eigenen Wirkungsbereiches, soweit die Daten ausschließlich oder überwiegend im Interesse der Gemeinde ermittelt oder verarbeitet werden.

Vollziehung

§ 32. Mit der Vollziehung dieses Bundesgesetzes sind, soweit sie nicht der Bundesregierung oder den Landesregierungen obliegt, der Bundeskanzler und die anderen Bundesminister nach Maßgabe des Bundesministeriengesetzes 1973 im Rahmen ihres Wirkungsbereiches betraut.

Erläuterungen

1. Allgemeines

1.1 Problemstellung

Die Diskussion über das Problem des „Datenschutzes" entstand mit dem vermehrten Einsatz der elektronischen Datenverarbeitung für die Sammlung von Daten und Informationen. Der Staat und Private müssen heute nicht nur aus Gründen der rationelleren Verwaltung, sondern auch auf Grund des Einsatzes von Planungsmethoden vermehrt auf Informationen zurückgreifen, und die Sammlung von Informationen in Datenbanken nimmt immer größeren Umfang an. Der rasche wissenschaftliche, technische, wirtschaftliche und soziale Fortschritt erzeugt auch eine immer größere Menge an Informationen, sodaß der erhöhten Nachfrage auch ein immer größeres Angebot an Informationen gegenübersteht. Diese Informationsmengen machen auch vor der Privatsphäre des Menschen nicht halt. Während bei einer mit herkömmlichen Mitteln geführten Datenbank diese Gefährdung der Privatsphäre wegen der schwierigen Handhabung umfangreicher Dateien noch relativ gering ist, gefährdet der Einsatz der modernen Technik im Hinblick auf die wesentlich leichtere Zugriffs- und Verbundmöglichkeit — man denke nur an die Anfragemöglichkeit in der Teleprocessing-Technik — zu den Daten die Privatsphäre in weitaus größerem Maße. Die Öffentlichkeit aber betrachtet jede technische Entwicklung, die den einzelnen gegenüber dem Staat transparenter macht, mit Skepsis. Aus dieser Einstellung heraus ist Zug um Zug mit der Entwicklung und dem Einsatz von EDV für die Speicherung von Daten persönlicher Natur die Forderung nach einem wirksamen Datenschutz erhoben worden.

Die Bestrebungen um einen „Datenschutz" haben nun das Ziel, durch legislative Maßnahmen die Freiheit und Privatsphäre physischer, zum Teil auch juristischer Personen gegenüber dem Mißbrauch von „personsbezogenen Daten" zu bewahren.

Der international übliche Begriff „Datenschutz" ist ungenau, da nicht nur „Daten" und „Datenträger" (dieser Teil des Datenschutzes wird allgemein als „Datensicherheit" bezeichnet) geschützt werden sollen, sondern vor allem Informationen über einen bestimmten Lebensbereich. Dieses sich auf das Grundrecht auf Schutz der Privatsphäre (Art. 8 der Europäischen Menschenrechtskonvention) berufende Anliegen muß gegenüber den Datenbanken der öffentlichen Hand seine Grenzen finden an den (anderen) Staatszwecken; gegenüber den privaten Datenbanken ist rechtspolitisch eine Abgrenzung zu den Grundrechten der Erwerbsfreiheit und der Informationsfreiheit (Art. 10 EMRK) sowie zu den wirtschaftlichen und technischen Möglichkeiten und Gegebenheiten zu suchen; Datenschutz bedeutet primär Datenverwendungskontrolle, nicht Datenverbot, mögliche Rationalisierungen sollen nicht verhindert werden.

Der vom Gesetzgeber eines Datenschutzgesetzes rechtspolitisch zu findende Ausgleich hat zwischen folgenden Interessenssphären zu geschehen (vgl. W. Steinmüller in: Datenbanken und Datenschutz, 1974, S. 114 ff.):

— Die menschlichen und gesellschaftlichen Freiheitsräume sollten durch die Entwicklung der Informationstechnologie nicht gefährdet werden.

— Die Funktionsfähigkeit von Staat, Wirtschaft und Wissenschaft muß durch EDV gehalten, ja gesteigert werden.

— Die Möglichkeiten der EDV müssen maximal genützt werden (aus Kostengründen, um die Effektivität der Rechtsordnung zu erhöhen, wegen der wachsenden Staatsaufgaben).

1.2 Die Arbeiten im Ausland

Ende der sechziger Jahre begann man sich zuerst im angloamerikanischen und im skandinavischen Rechtskreis mit diesen Fragen zu beschäftigen, wobei neben den ersten wissenschaftlichen Arbeiten vor allem eine Bestandaufnahme durch von den Regierungen der USA, Großbritanniens, Schwedens, Dänemarks und Kanadas eingesetzte Kommissionen erfolgte, die in ihren Berichten die tatsächliche Situation beschrieben, Bedrohungen aufzeigten und legistische Maßnahmen vorschlugen. Inzwischen ist nicht nur die rechtswissenschaftliche Literatur zum Thema Datenschutz fast unübersehbar geworden (für

Österreich vgl. etwa G. Mutz, Rechtsprobleme des sogenannten Datenschutzes, Juristische Blätter 1973, S. 245—255; G. Stadler, Rechtsprobleme beim Einsatz von EDV-Anlagen in Unternehmen, österreichische Zeitschrift für Wirtschaftsrecht, 1974/2; G. Stadler, Hrsg., Datenschutz, 1975; L. Reisinger, Zur Problematik des Datenschutzes, Österreichische Juristen-Zeitung 1975, S. 115 bis 125; W. Dohr, Datenschutz in Österreich, Öffentliche Verwaltung und Datenverarbeitung 1974/11; für das deutschsprachige Ausland vor allem die einschlägigen Aufsätze in den Fachzeitschriften „Öffentliche Verwaltung und Datenverarbeitung" und „Datenverarbeitung im Recht"), es werden in der Mehrzahl der westlichen Industriestaaten auch bereits Gesetzentwürfe erörtert; abgesehen von Gesetzen für Detailbereiche in den USA (Fair Credit Reporting Act 1970) und in einzelnen deutschen Bundesländern (Hessen, Rheinland-Pfalz, Bayern) ist aber nur in Schweden ein allgemeines Datenschutzgesetz bereits erlassen (Datalag vom 11. Mai 1973) und am 1. Juli 1974 in Kraft getreten.

In den USA wurde am 31. Dezember 1974 ein „Privacy Act" für Bereiche der öffentlichen Verwaltung erlassen. Diese Gesetze bzw. Entwürfe (Bundesrepublik Deutschland, Norwegen, Neuseeland, Belgien, einige Schweizer Kantone und andere) beziehen sich teils nur auf Datenbanken der öffentlichen Hand, teils nur auf solche der privaten Bereiche (so der Fair Credit Reporting Act 1970), teils auf alle Datenbanken.

Besonders ist hinzuweisen auf den gegenwärtigen im deutschen Bundestag in Verhandlung stehenden Entwurf eines Gesetzes zum Schutze von Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz) vom 21. September 1973 (Drucksache des Bundestages 7/1027). Diese Regierungsvorlage, zu der inzwischen vom Bundesrat Stellung genommen wurde, und über die mehrere Hearings abgehalten wurden (vgl. Zur Sache, Themen parlamentarischer Beratung, Bonn, 5/74), wird auf drei Bereiche anzuwenden sein: Datenverarbeitung in Bundesstellen und von Privaten für eigene und fremde Zwecke. Eine Besonderheit des deutschen Entwurfes ist die Einrichtung eines Datenschutzbeauftragten für nichtöffentliche Stellen, die die Datenverarbeitung für eigene Zwecke betreiben. Dieser Datenschutzbeauftragte ist unmittelbar dem Geschäftsführer bzw. Vorstand des Unternehmens unterstellt und hat die Einhaltung der Datenschutzvorschriften sicherzustellen. Private, die gesetzmäßig die Verarbeitung personenbezogener Daten für Dritte durchführen, haben dies einer Aufsichtsbehörde zu melden, die ein entsprechendes Register zu führen hat. Für den öffentlichen Bereich sieht der deutsche Entwurf keine Aufsichtsbehörde bzw. Stelle vor, bei der der einzelne seine Rechte (Benachrichtigung jeder Person, über die erstmals Daten gespeichert werden) gegenüber der datenverarbeitenden Verwaltung geltend machen kann. Der Entwurf nimmt vom Datenschutz weiters grundsätzlich aus die sogenannten „freien Daten" (Name, Geburtsdatum, Beruf, Anschrift, Telefonnummer) und Daten und Datenverarbeitung, die aus Gründen des Staatsinteresses geheimzuhalten sind (z. B. Bundeskriminalamt, Bundesnachrichtendienst). Zum Großteil betreffen die erwähnten Dokumente nicht nur die EDV-unterstützte Datenbank, sondern auch die konventionell geführte Datensammlung.

Hinzuweisen ist auch auf den in Großbritannien zunächst gewählten Weg des Datenschutzes, der hauptsächlich von der Berufsvereinigung des bei Datenverarbeitungsanlagen beschäftigten Personals, der British Computer Society, getragen wird, in deren Rules of Conduct und im Code of Good Practice Grundsätze des Datenschutzes enthalten sind, zu deren Einhaltung sich die Mitglieder der Gesellschaft bei sonstiger disziplinärer Verantwortlichkeit gegenüber der Gesellschaft verpflichten. Aber auch in Großbritannien wurde jüngst erkannt, daß eine derartige freiwillige Berufsdisziplin wohl nicht für einen effektiven Datenschutz ausreiche.

Auch die OECD (Computer Utilisation Group, Arbeitsgruppe Datenbanken), die Vereinten Nationen (vgl. Doc. E./CN. 4/1028 Add. 3 und 1068) und der Europarat beschäftigen sich mit dem Problem des Datenschutzes. Von einem Expertenkomitee des Europarates wurden 2 Entwürfe ausgearbeitet, die vom Ministerkomitee des Europarates als Entschließungen verabschiedet wurden:

Die Resolution über den Schutz der Privatsphäre physischer Personen in Anbetracht der Verwendung elekronischer Datenbanken in privatem Bereich [Res. (73) 22] und die Resolution über den Schutz der Privatsphäre physischer Personen in Anbetracht der Anwendung elektronischer Datenbanken im öffentlichen Bereich [Res. (74) 29].

Letztere Resolution hat samt ihrem Anhang in einer inoffiziellen deutschen Übersetzung folgenden Wortlaut:

„Das Ministerkomitee des Europarates, in der Erwägung, daß es das Ziel des Europarates ist, zwischen seinen Mitgliedern eine größere Einheit herzustellen;

im Wunsche, zum allgemeinen Verständnis und Vertrauen beizutragen in Anbetracht der neuen Methoden der Verwaltung, die öffentliche Stellen in den Mitgliedsstaaten anwenden, um die ihnen übertragenen Verwaltungsaufgaben ordentlich durchzuführen;

erkennend, daß der Gebrauch von elektronischen Datenbanken durch öffentliche Stellen An-

laß gegeben hat für Überlegungen über den weiteren Schutz der Privatsphäre physischer Personen;

in der Erwägung, daß die Annahme allgemeiner Grundsätze in diesem Gebiet zu einer Lösung dieses Problems in den Mitgliedstaaten führen und helfen kann, ungerechtfertigte Unterschiede in diesem Gebiet zwischen den Gesetzgebungen der Mitgliedstaaten zu verhindern;

in Erinnerung an seine Resolution (73) 22 über den Schutz der Privatsphäre physischer Personen gegenüber der Anwendung elektronischer Datenbanken im privaten Bereich;

im Bewußtsein des Art. 8 der Konvention über den Schutz der Menschenrechte und Grundfreiheiten,

empfiehlt den Regierungen der Mitgliedsstaaten:

a) alle Maßnahmen zu treffen, die sie für notwendig erachten, um die im Annex dieser Resolution niedergelegten Prinzipien wirksam zu machen;

b) zu gegebener Zeit dem Generalsekretär des Europarates über die in diesem Gebiet vorgenommenen Maßnahmen zu informieren.

Annex

Die folgenden Prinzipien sind anzuwenden auf personenbezogene Informationen, die in elektronischen Datenbanken des öffentlichen Bereiches gespeichert sind. Im Sinne dieser Resolution bedeutet ‚personenbezogene Informationen' Informationen, die sich auf Individuen (physische Personen) beziehen und ‚elektronische Datenbank' bedeutet jede elektronische Datenverarbeitungsanlage, die für die Verarbeitung derartiger Informationen verwendet wird.

1. Grundsätzlich soll die Öffentlichkeit regelmäßig informiert werden über die Einrichtung, Verwendung und Entwicklung von elektronischen Datenbanken im öffentlichen Bereich.

2. Die gespeicherten Informationen sollen

a) erhoben werden durch gesetzmäßige und sachlich gerechtfertigte Mittel;

b) richtig sein und auf dem laufenden gehalten werden;

c) für den Zweck, für den sie gespeichert werden, geeignet und von Bedeutung sein.

Jede Sorgfalt soll auf die Berichtigung unrichtiger Informationen und auf die Löschung ungeeigneter, unbeachtlicher oder überholter Informationen gelegt werden.

3. Insbesondere wenn in elektronischen Datenbanken Informationen aus der Intimsphäre physischer Personen verarbeitet werden oder wenn die Datenverarbeitung zu unsachlicher Diskriminierung führen kann,

a) muß ihre Einrichtung durch Gesetz vorgesehen sein oder durch eine besondere Verordnung oder in einem Dokument in Übereinstimmung mit dem Rechtssystem des Mitgliedsstaates kundgemacht sein;

b) dieses Gesetz, diese Verordnung oder die sonstigen Vorschriften müssen klar den Zweck der Speicherung und den Gebrauch dieser Informationen angeben, ebenso die Voraussetzungen, unter denen diese Informationen weitergegeben werden, entweder innerhalb der öffentlichen Verwaltung oder an private Personen oder Institutionen;

c) die gespeicherten Daten dürfen nicht für andere Zwecke verwendet werden als die angegebenen, ausgenommen eine Ausnahme ist ausdrücklich im Gesetz vorgesehen oder von einer zuständigen Behörde bewilligt worden oder die Vorschriften über die elektronische Datenbank wurden geändert.

4. Bestimmungen sollen festgelegt werden, um Zeitgrenzen anzugeben, jenseits derer bestimmte Kategorien von Informationen nicht mehr gespeichert oder benützt werden dürfen.

Ausnahmen von diesem Grundsatz sind jedoch zulässig, wenn der Gebrauch der Informationen für statistische, wissenschaftliche oder historische Zwecke ihre Aufbewahrung für unbestimmte Dauer erfordert. In diesem Fall müssen Vorkehrungen getroffen werden, um sicherzustellen, daß die Privatsphäre der betroffenen Personen nicht verletzt wird.

5. Jede Person soll das Recht erhalten, die über sie gespeicherte Information zu erfahren. Jede Ausnahme von diesem Grundsatz oder Beschränkung der Ausübung dieses Rechtes muß genau geregelt sein.

6. Vorkehrungen sollen getroffen werden gegen jeden zweckwidrigen oder mißbräuchlichen Gebrauch von Informationen. Zu diesem Zweck

a) muß jedermann, der mit der Handhabung elektronischer Datenverarbeitung befaßt ist, durch Verhaltensregeln gebunden sein, die eine mißbräuchliche Datenverwendung verhindern und insbesondere eine Verschwiegenheitspflicht enthalten sollen;

b) müssen elektronische Datenbanken mit einem Sicherungssystem ausgerüstet sein, das den Zugriff zu den Datenbanken verhindern soll für Personen, die nicht zum Erhalt solcher Informationen berechtigt sind, und das Vorkehrungen enthalten muß für die Entdeckung von Fehlleitungen von Informationen, seien sie vorsätzlich oder nicht.

7. Der Zugang zu nicht allgemein erhältlichen Informationen soll auf die Personen beschränkt sein, deren Tätigkeit sie berechtigt, von diesen

Informationen zum Zwecke der Vollziehung ihrer Obliegenheiten Kenntnis zu erlangen.

8. Wenn Informationen für statistische Zwecke verwendet werden, dürfen sie nur in einer Form ausgegeben werden, die es unmöglich macht, die Informationen auf eine bestimmte Person zu beziehen."

Ein österreichischer Vertreter hat nicht nur an der Ausarbeitung dieser Resolutionen mitgewirkt, sondern es wurde auch bei der Ausarbeitung dieser Vorlage eines Datenschutzgesetzes auf die Grundsätze der Resolution Bedacht genommen und die Erfahrungen und Diskussionen in den Mitgliedstaaten des Europarates berücksichtigt.

1.3. Die Grundsätze des Datenschutzrechtes

Allgemein wird anerkannt, daß ein wirksamer Datenschutz nicht allein durch freiwillige Selbstbeschränkung, sondern nur durch rechtliche Maßnahmen erzielt werden kann. Aus den nationalen und internationalen Dokumenten lassen sich rechtsvergleichend folgende Grundsätze für ein Datenschutzrecht ableiten:

— Der Grundsatz der **Weitergabebeschränkung:**

Die Weitergabe „personsbezogener Daten" (dieser Begriff findet sich zwar in der Mehrzahl der angeführten Dokumente, seine Abgrenzung ist aber strittig) ist, wenigstens bei öffentlichen Datenbanken, in der Regel nur kraft ausdrücklicher gesetzlicher Ermächtigung zulässig (auch hinsichtlich der Speicherung ist in der Mehrzahl der Entwürfe eine derartige gesetzliche Ermächtigung notwendig), und die Daten dürfen nur zu dem Zweck verwendet werden, zu dem sie gespeichert wurden; bei privaten Datenbanken ergibt sich die Weitergabebeschränkung aus dem Unternehmungszweck und aus den Wirtschaftsgesetzen.

— Der Grundsatz der **Relevanz** der gespeicherten Daten:

Die gespeicherten Daten sollen in einer Beziehung zu dem Zweck stehen, für den sie gespeichert wurden; es sollen nicht willkürlich Daten über eine beliebige Personengruppe gespeichert werden dürfen oder in verschiedenen Datenbanken gespeicherte Daten über dieselbe Person beliebig verbunden werden. Für öffentliche Datenbanken ergibt sich damit die Relevanz aus der Vollziehungszuständigkeit der Behörde, für private Datenbanken aus dem Unternehmensgegenstand. Irrelevante Daten sind zu löschen.

— Der Grundsatz der **Richtigkeit** der Daten:

Wenngleich die Träger der Datenbanken nicht verpflichtet sind, die zu speichernden Informationen auf ihre Richtigkeit hin zu überprüfen, so sind sie doch verpflichtet, bei Zweifeln über deren Richtigkeit Nachforschungen anzustellen, sie gegebenenfalls zu berichtigen sowie die Daten vollständig und auf dem laufenden zu halten und überholte Daten auszuscheiden. Personen, die Kenntnis über unrichtige, sie betreffende Daten erhalten, steht ein Berichtigungsanspruch zu.

— **Der Publizitätsgrundsatz**

Die Allgemeinheit bzw. die Personen, über die Informationen gespeichert sind, müssen die Möglichkeit haben, zu erfahren, in welchen Datenbanken personenbezogene Informationen gespeichert sind, wer Zugang zu ihnen hat und zu welchem Zweck sie verwendet werden. Diesem Gedanken wird Rechnung getragen durch die Pflicht, Datenbanken mit personenbezogenen Informationen einer Stelle zu melden. Diese Stelle führt in der Regel ein öffentlich zugängliches Datenbankregister. Zu dieser generellen Publizität kommt die individuelle, nämlich das Recht des Betroffenen auf Kenntnis der über ihn gespeicherten Daten sowie über deren Weitergabe an Dritte: Die Datenbank muß ihm Auskunft erteilen. Eine Beschränkung des Auskunftsrechtes ist in der Regel bei Daten vorgesehen, die aus öffentlichen oder überwiegenden Interessen Dritter geheimzuhalten sind.

— der Grundsatz der **Fremdaufsicht:**

Die oben erwähnten Dokumente gehen von einer doppelten Kontrolle der Datenbanken aus: einerseits durch den Betroffenen auf Grund des ihm zustehenden Auskunftsrechtes, andererseits ist angesichts der Überforderung der individuellen Möglichkeiten eine Institution vorgesehen, die die Einhaltung der Datenschutzbestimmungen zu überwachen hat und an die die Betroffenen ein Antragsrecht haben. Diese Fremdkontrolle wird ausgeübt durch eine von der übrigen Verwaltung getrennte Aufsichtsbehörde („Datenschutzbeauftragter" in Hessen, „Datainspektionen" in Schweden). Den Aufsichtsbehörden steht nicht nur ein Einsichtsrecht in allen ihnen unterstellten Datenbanken sowie deren Registrierung zu, sie sind zum Teil auch Entscheidungsinstanz in allen Fragen betreffend die Zulässigkeit einer Datenbank.

— Der Grundsatz der **erhöhten Berufspflichten** für EDV-Personal:

Das in Datenbanken beschäftigte Personal soll durch ein allgemeines gesetzliches Berufsgeheimnis zur Verschwiegenheit verpflichtet sein. Geheimnisbruch wird unter Strafsanktion gestellt.

Diese Grundsätze finden sich in einer für die österreichische Rechtsordnung modifizierten Form sowohl in der Regierungsvorlage eines Datenschutzgesetzes als auch in dem am 11. Juni 1974 im Nationalrat eingebrachten Initiativantrag der Österreichischen Volkspartei für ein Bundesver-

fassungsgesetz über allgemeine Regeln auf dem Gebiete des Datenschutzes und der Datensicherung (II-3586 der Beilagen zu den stenographischen Protokollen des Nationalrates, XIII. GP).

1.4 Die Vorarbeiten für ein Datenschutzgesetz in Österreich

Auch Österreich hat der oben beschriebenen internationalen Entwicklung Rechnung getragen und bereits 1971 im Rahmen des Koordinationskomitees für die elektronische Datenverarbeitung im Bereiche des Bundes unter dem Vorsitz des Bundeskanzleramtes — Verfassungsdienst eine Arbeitsgruppe „Datenschutz" eingesetzt. Auf Grund der Beratungen dieser Arbeitsgruppe wurde ein erster Vorentwurf für ein Datenschutzgesetz am 20. Feber 1973 erstellt, der eine verfassungsgesetzliche Verankerung des Schutzes der Privatsphäre gegenüber ihrer Bedrohung durch Datensammlungen vorsah. Zu diesem Entwurf wurde zunächst die Auffassung der unmittelbar berührten Bundesministerien für Finanzen, für Handel, Gewerbe und Industrie, für Inneres, für Justiz, für Landesverteidigung und für soziale Verwaltung gehört. Das Ergebnis dieser ersten Kontaktnahme, das die Notwendigkeit eines allgemeinen Datenschutzgesetzes zum Teil in Zweifel gezogen hat und im übrigen zu wesentlichen Fragen des Datenschutzes zu zum Teil kontroversellen Meinungen geführt hat, hat das Bundeskanzleramt — Verfassungsdienst veranlaßt, am 1. August 1973 einen zweiten Referentenentwurf einem allgemeinen Begutachtungsverfahren zuzuleiten, der ein anderes Konzept verfolgte als der 1. Entwurf, sich nur auf Datenbanken des Bundes beschränkte, von einer Verfassungsbestimmung absah, einen Datenschutzbeauftragten je Datenbank und ein Aufsichtsrecht der Volksanwaltschaft vorsah.

Die Ergebnisse dieses Begutachtungsverfahrens waren im Detail widersprüchlich, doch läßt sich eine allgemeine Tendenz feststellen:

— Die Initiative zur Erlassung eines Datenschutzgesetzes wurde begrüßt und die damit auftretenden Schwierigkeiten werden anerkannt.

— Der Geltungsbereich des Entwurfes, der sich nur auf Dateien von Einrichtungen des Bundes bezog, wurde allgemein als zu eng abgelehnt; eine Einbeziehung wenigstens der Datenbanken der Länder, der Gemeinden und der Selbstverwaltungskörper wurde verlangt. Einbezogen werden soll auch die Datenverarbeitung, die im Auftrag der öffentlichen Hand von Privaten vorgenommen wird. Einer Verfassungsbestimmung zugunsten des Bundes steht man allgemein positiv gegenüber, sogar seitens einzelner Bundesländer.

— Soweit auf den grundrechtlichen Datenschutz Bezug genommen wurde, wurde anerkannt, daß dieser einerseits durch Art. 8 EMRK wenigstens teilweise gewahrt ist, und andererseits, daß er bei einer Neufassung der Grundrechte berücksichtigt werden müsse.

— Der Begriff der Datenbank, der auf Grund des Entwurfes „eine nach bestimmten Merkmalen geordnete Sammlung von Daten, die nach anderen bestimmten Merkmalen umgeordnet oder ausgewertet werden kann" betrifft, wurde als zu weit abgelehnt. Eine Berücksichtigung auch der nichtautomatisierten Register wurde zwar bejaht, doch wäre der Datenschutz nur ab einem größeren Umfang der Datei relevant.

— Die Verwendung des Begriffes „personenbezogene Daten" wurde zwar allgemein als problematisch angesehen, doch bietet sich dafür keine Alternative an.

— Eine besondere, von den meisten Stellungnahmen behandelte Problematik ergibt sich aus der Verfassungsbestimmung des Art. 22 B-VG, die die Organe des Bundes, der Länder und der Gemeinden im Rahmen ihres gesetzlichen Wirkungsbereiches zur wechselseitigen Hilfe verpflichtet (soweit das Amtsgeheimnis nicht entgegensteht). Die besonders die Privatsphäre bedrohende Integration von Datenbanken und die Kumulierung von Informationen kann damit im Einzelfall nicht verhindert werden.

— Einem Datenschutzbeauftragten wurde allgemein nur unter der Voraussetzung zugestimmt, daß er weisungsfrei gestellt bzw. der gesetzgebenden Gewalt zugeordnet ist.

— Ein Auskunftsrecht für Abgeordnete über Individualdaten wurde einhellig abgelehnt.

Auf Grund der Ergebnisse dieses Begutachtungsverfahrens und des gegebenen parlamentarischen Interesses — wie mehrere Anfragen an den Herrn Bundeskanzler zeigten — wurde vom Bundeskanzleramt — Verfassungsdienst am 16. Mai 1974 ein revidierter Entwurf eines Datenschutzgesetzes zur Begutachtung versendet (GZ 51.500-2 d/74), der bei grundsätzlicher Beibehaltung der Struktur des Entwurfes vom 1. August 1973 der allgemeinen Tendenz der beteiligten Stellen nach einer Ausweitung des Geltungsbereiches des Gesetzes entgegenkam, wesentliche Detailanregungen aufgriff, die von einzelnen Stellen gemacht wurden, und auch die jüngste internationale Erfahrung berücksichtigte.

Im folgenden werden — abgesehen von verfahrensrechtlichen Bestimmungen — die wesentlichen Unterschiede zwischen dem Entwurf vom 16. Mai 1974 und der Regierungsvorlage dargestellt:

Der Entwurf enthielt eine Verfassungsbestimmung, die den Geltungsbereich des Bundes-

Datenschutzgesetzes auch auf die von den Ländern geführten Datenbanken erstreckte bis die Länder dem Bundes-Datenschutzgesetze entsprechende Gesetze erlassen haben. Hinsichtlich der unmittelbar bei Dienststellen und Behörden des Bundes eingerichteten Datenbanken stützte sich der Entwurf auf die Bundeskompetenz in Gesetzgebung und Vollziehung gemäß Art. 10 B-VG, insbesondere Art. 10 Abs. 1 Z. 16 B-VG. Während man grundsätzlich die Datensammlung und die Datenspeicherung für und im Zusammenhang mit einer bestimmten Verwaltungsmaterie kompetenzrechtlich als Annex zur betreffenden Verwaltungsmaterie (z. B. Sozialversicherungswesen, Art. 10 Abs. 1 Z. 11 B-VG) ansehen kann (vgl. VfGH. Slg. 4106/1961) und sich die Zulässigkeit des Aufbaues von konventionellen oder EDV-unterstützten Datenbanken aus der Organisationsgewalt der Verwaltung ergibt, sind Bestimmungen über die Einrichtung und den Umfang von Datenbanken bei Bundesbehörden als Bundesdienststellen dem Kompetenztatbestand „Einrichtung der Bundesbehörden und sonstigen Bundesämter" (Art. 10 Abs. 1 Z. 16 B-VG) zuzuordnen. Die mit hoheitlichen Mitteln vorgenommene Datensammlung bedarf bereits bisher einer gesetzlichen Ermächtigung (als Beispiel sei auf das Bundesstatistikgesetz 1965 hingewiesen), für die innere Organisation und die Handhabung der Datensammlung bestanden bisher keine gesetzlichen Ermächtigungen, wenn man von Geheimhaltungsvorschriften absieht.

Der Begriff der Datenbank bezog sich auch auf konventionell geführte Datenbanken, sofern in ihnen mindestens 5000 personenbezogene Daten oder über mehr als 100 Betroffene mindestens je zehn personenbezogene Daten gespeichert sind. Auf eine Einbeziehung von privaten Datenbanken unter den Entwurf wurde zunächst verzichtet, da die hiefür zu erlassenden Bestimmungen im Detail einen wesentlich anderen Inhalt haben müßten als die für öffentliche Datenbanken vorgesehenen und mit dem Recht der Wirtschaftsaufsicht im Zusammenhang stehen. An die mit der Aufsicht über private Unternehmen unmittelbar befaßten Bundesministerien wurde aber anläßlich des Begutachtungsverfahrens das Ersuchen um Stellungnahme gerichtet, ob die gegebenen rechtlichen Bestimmungen ausreichen, um der unzweifelhaft gegebenen Bedrohung der Privatsphäre durch private Datenbanken zu begegnen.

Weiters wurde im Zuge dieses Begutachtungsverfahrens eine erste Erhebung über bereits bestehende oder in Planung befindliche Datenbanken im Bundes- und Landesbereich durchgeführt, um sich über den sachlichen Geltungsbereich und die Tragweite des Entwurfes zu informieren. Dies ergab nicht nur Hinweise auf die konkret zu erwartenden Probleme, auf die sich aus einem Datenschutz ergebenden Kosten, auf Unschärfen bzw. unterschiedlichen Auslegungen der Begriffsbestimmungen, sondern auch erstmals eine Übersicht über die tatsächlich bereits vorhandenen Datenbanken, ihren Inhalt und ihren Zweck sowie den Kreis der von ihnen betroffenen Personen (eine Schätzung über das Ausmaß der „Verdatung" in Österreich findet sich auch in: Der Bürger in der Informationsgesellschaft, Materialien zum Datenschutz in Österreich; herausgegeben von der Österreichischen Gesellschaft für Politik, 1974).

Von den Bundesministerien werden derzeit zirka 200 Datenbanken geführt, die die Kriterien des Entwurfes vom 16. Mai 1974 erfüllten, wobei das Schwergewicht im Bundesministerium für soziale Verwaltung und im Bundesministerium für Finanzen liegt. Zunehmend werden diese Datenbanken auf EDV umgestellt. In den Bundesländern schwankt die Zahl zwischen je 20 und 100, je nach Organisation der Bezirksverwaltungsbehörden.

1.5 Die Ergebnisse des Begutachtungsverfahrens zum Entwurf vom 16. Mai 1974

Das Begutachtungsverfahren zum Entwurf, das mit 30. Juli 1974 befristet war, hat bei einhelliger Bejahung der Notwendigkeit eines Datenschutzgesetzes und neben einer Fülle detaillierter Anregungen und Kriterien vor allem zu folgenden Problemen Aussagen ergeben:

a) **Geltungsbereich**

aa) Die Einbeziehung aller Datenbanken der öffentlichen Hand wurde begrüßt.

bb) Die Nichteinbeziehung auch der privaten Datenbanken wurde von fast allen Stellen als wesentlicher Mangel des Entwurfes angesehen. Seitens des Bundesministeriums für Finanzen wurden nachdrücklich Schutzbestimmungen auch gegen Datenbanken der Kreditinstitute und der Versicherungen gefordert, da die bestehenden Gesetze unzureichend sind. Das Bundesministerium für Handel, Gewerbe und Industrie vermeinte, daß die in Kraft getretenen Bestimmungen der neuen Gewerbeordnung die Möglichkeit der Verhinderung des Datenmißbrauches böten.

b) **Kompetenz**

aa) Das Ausgehen des Entwurfes von Art. 10 Abs. 1 Z. 16 B-VG (Organisation der Bundesbehörden) als Kompetenzgrundlage für die Erlassung eines Bundes-Datenschutzgesetzes wurde von einigen der begutachtenden Stellen als im Hinblick auf die Versteinerungs-

theorie des Verfassungsgerichtshofes nicht unbedenklich angesehen, da „Datenschutz" dem Verfassungsgesetzgeber des Jahres 1925 unbekannt war.

b) Während seitens einzelner Stellen des Begutachtungsverfahrens eine eigene, umfassende Bundeskompetenz gefordert wurde (z. B. Arbeiterkammertag), lehnten die Bundesländer zum überwiegenden Teil die im § 4 des Bundes vorgesehene auflösend bedingte Kompetenzbestimmung ab, da sie die Datenschutzgesetze der Länder auch inhaltlich so vorbestimmen würde, daß ihnen materiell kein Spielraum bliebe. Es wird aber auch seitens der Länder die Notwendigkeit einheitlicher Datenschutzbestimmungen anerkannt. In einigen Stellungnahmen fand sich die Anregung, den Datenschutz zum Gegenstand von Vereinbarungen nach Art. 15 a B-VG (in der Fassung BGBl. Nr. 444/1974) zu machen.

c) Die Ausdehnung des Datenschutzgesetzes auch auf **manuell geführte Datenbanken** wurde zwar nicht allgemein abgelehnt, doch wird auf eine Fülle von Schwierigkeiten bei der Vollziehung hingewiesen (z. B. seitens des Bundesministeriums für Finanzen), auch darauf, daß derartige Datensammlungen schon längst bestehen, ohne daß ein besonderes Schutzbedürfnis zu vermerken ist. Bei der Einschränkung auf EDV-Datenbanken könnte auch von den in vielen Stellungnahmen abgelehnten ziffernmäßigen Definitionselementen abgesehen werden.

d) Zur grundsätzlichen **rechtstechnischen Konzeption des Entwurfs,** die von einem Sonderverfahren für alle Verletzungen des Datenschutzgesetzes ausgeht, wobei die Datenschutzkommission unzweifelhaft auch die Bestimmung des Art. 8 EMRK anzuwenden hat, womit diese Bestimmung für Österreich erstmalig inhaltlich determiniert würde, nahmen besonders die Österreichische Rektorenkonferenz und die Bundeskammer der gewerblichen Wirtschaft Stellung. Die Rektorenkonferenz schlägt eine Zuständigkeit der Datenschutzkommission nur für jene Fälle vor, in denen eine Verletzung des Datenschutzgesetzes unabhängig von einem konkreten Verwaltungsverfahren erfolgt (denn für Verletzungen im Rahmen eines durch Bescheid abgeschlossenen Verwaltungsverfahrens sei der übliche Verwaltungsrechtszug bis zum Verwaltungsgerichtshof und zum Verfassungsgerichtshof ausreichend).

Die Bundeskammer der gewerblichen Wirtschaft schlägt vor, den Datenschutz durch Ausbau des Immaterialgüterrechtes zu gewährleisten: Der einzelne soll an den auf ihn bezogenen Daten private Rechte haben, die allenfalls auch verfassungsgesetzlich gewährleistet sein könnten, gegen deren Verletzung er sich mit den herkömmlichen Mitteln — bei Verletzung im Rahmen hoheitlicher Tätigkeiten: Beschwerde beim Verfassungsgerichtshof, allenfalls auch Amtshaftungsanspruch; bei Verletzung nichthoheitlicher Tätigkeiten, sei es durch den Staat, sei es durch einen Privaten, Feststellungsanklage, Unterlassungsklage, allenfalls Schadenersatzanspruch — zur Wehr zu setzen hätte. Diese herkömmliche Rechtsbehelfe könnten durch neue ergänzt werden, die sich aber im Rahmen des überkommenen Rechtsschutzsystems halten könnten, etwa: Feststellungsbescheid, Verwaltungsgerichtshofbeschwerde gegen rechtsverletzende hoheitliche Akte, mögen diese auch keine Bescheide sein (Vorbild: Beschwerden gegen faktische Amtshandlungen beim Verfassungsgerichtshof). Eine weitere Ergänzung wären strafrechtliche Sanktionen gegen Datenmißbrauch jeder Art. Dieses Konzept hätte den Vorteil, daß es sich in das überkommene Rechtsschutzsystem einordnen und auch die anderen Datenbanken erfassen würde.

e) Ein besonderer **grundrechtlicher Datenschutz** wurde im Begutachtungsverfahren nur von wenigen Stellen gefordert.

f) Die Stellungnahmen zu dem vom Entwurf vorgesehenen **Voraussetzungen für den zulässigen Aufbau einer Datenbank** waren divergierend:
Während von einigen Stellen ein Gesetz (in formellem Sinn) als Voraussetzung für eine Datenbank gefordert wurde, setzten sich andere (bes. die Bundesministerien) für eine Streichung des Wortes „unmittelbar" in § 6 des Entwurfes ein, sodaß eine Datenbank auch schon dann erlaubt wäre, wenn sie für den Rechtsträger zur Wahrnehmung der im Gesetz übertragenen Aufgaben eine (mittelbare oder unmittelbare) Voraussetzung ist.

g) In gleicher Weise divergierten die Stellungnahmen zur Frage der zulässigen **Verbindung (Verknüpfung) von Daten,** wobei aber mehrheitlich auch die einmalige Verbindung von Daten als für den Datenschutz beachtlich angesehen wird (nicht nur die dauernde Verbindung von personenbezogenen Daten).

h) Gegen den **Schutz auch juristischer Personen** wurde nicht Stellung genommen, seitens der Bundeskammer wurde ein Schutz auch der Handelsgesellschaften gefordert.

i) Der Entwurf ging davon aus, daß auch die **Datenbanken gesetzlich anerkannter Kirchen und Religionsgemeinschaften** unter seinen Geltungsbereich fallen, was von diesen scharf abgelehnt wird, da ihnen damit die Führung von Datenbanken zwecks Evidenthaltung der Beitragsleistungen ihrer Mitglieder untersagt würde.

j) Im Zusammenhang damit findet sich in mehreren Stellungnahmen (z. B. Salzburger Landesregierung, Rektorenkonferenz) in Anlehnung an den Entwurf der deutschen Bundesregierung der Vorschlag, im Gesetz taxativ **freie Daten** aufzuzählen, die nicht dem Datenschutz unterliegen. Als solche freie Daten kommen in Betracht: Name, Geburtsdatum, Adresse, Tel.-Nr.

k) Seitens der Bundeswirtschaftskammer wurde ein Verbot der Verwendung **ausländischer Datenbanken** gefordert, eine Forderung, die in der internationalen Datenschutzdiskussion wesentlich breiteren Raum einnimmt.

l) Die Notwendigkeit der Erlassung von **Datenbank-Betriebsordnungen** wurde einhellig begrüßt, wobei aber nähere inhaltliche Determinierungen schon im Gesetz und eine Vorkehrung für möglichst einheitliche Bestimmungen gefordert werden.

m) Der Einrichtung von **Datenschutzkommissionen** wurde gegenüber Datenschutzbeauftragten, die im Vorentwurf vorgesehen waren, eindeutig der Vorzug gegeben. Zur Zusammensetzung der Datenschutzkommissionen wird zum Teil im Hinblick auf ein Vorschlagsrecht der Interessenvertretungen, der Datenschutzkommissionen selbst bzw. des Nationalrates Stellung genommen, zur Zuständigkeit wird auch für eine begutachtende bzw. amtswegige Tätigkeit votiert. Die Österreichische Richtervereinigung regte an, einen Rechtszug an den Verwaltungsgerichtshof auszuschließen.

n) Eine **Popularbeschwerde** an die Datenschutzkommission, unabhängig von der Verletzung eigener Rechte, wird einhellig abgelehnt, ebenso ein **Einsichtsrecht für Abgeordnete** in Datenbanken der Vollziehung.

1.6 Die Ausarbeitung der Regierungsvorlage vom 16. Dezember 1975

Die Regierungsvorlage vom 16. Dezember 1974, mit der die Bundesregierung einen Programmpunkt der Regierungserklärung vom 5. November 1971 erfüllte, nahm auf die Ergebnisse der Begutachtungsverfahren, auf die mit den Vertretern einzelner Bundesministerien geführten Gespräche sowie auf die internationalen Erfahrungen beim Schutz der Privatsphäre gegen ihre Bedrohung und Verletzung durch Datenbanken Bedacht. Angesichts der Schwierigkeiten der Materie war es teilweise unmöglich, die Meinungen aller begutachtenden Stellen zu einem Kompromiß zu formulieren, und es müßte ein Ausgleich gesucht werden zwischen den berechtigten Interessen der Verwaltung auf Information und auf ökonomischen EDV-Einsatz und dem in Gedanken des freiheitlichen Rechtsstaates gegründeten unverletzbaren Freiheitsraum jeder Person.

Die gegenüber dem mit der GZ 51.500-2 d/74 vom Bundeskanzleramt am 16. Mai 1974 zur Begutachtung versendeten Entwurf wesentlichen Änderungen sind:

a) unmittelbare Anwendbarkeit des Datenschutzgesetzes mit Verfassungsbestimmung auf alle Datenbanken der öffentlichen Hand, wobei die Vollziehung des Gesetzes für die Datenbanken der Länder und Gemeinden den Ländern obliegt.

b) Die Berechtigung zur Erhebung und Verarbeitung personenbezogener Daten soll auf eine gesetzliche Grundlage oder auf den Zweck der Verarbeitung bzw. auf die Aufgaben der verarbeitenden Behörde abgestellt werden.

c) Einbeziehung der privaten Datenbanken unter ein Aufsichtsrecht, das im Rahmen der allgemeinen Gewerbe-, Kredit-, Vereins- und Versicherungsaufsicht ausgeübt werden soll. (Daß der Geltungsbereich des Datenschutzes sich auch auf private Datenbanken erstrecken soll, war ein fast einhelliger Wunsch der begutachtenden Stellen.)

d) Einschränkung des Gesetzes auf Datenbanken, die mit EDV oder vergleichbaren Techniken geführt werden.

e) Aufnahme einer Bestimmung gegen die Umgehung des Gesetzes durch im Ausland gelegene Datenverarbeitungsanlagen.

f) Verschiedene Bestimmungen, um die mit dem Datenschutz notwendigen Verwaltungsverfahren möglichst sparsam zu gestalten.

g) Detaillierte Bestimmungen über die Datenbank-Verordnung.

Zur Behandlung dieser Regierungsvorlage und eines Initiativantrages der ÖVP für ein Bundesverfassungsgesetz, womit allgemeine Regelungen auf dem Gebiet des Datenschutzes und der Datensicherung getroffen werden, vom 11. Juni 1974, der in etwa von den gleichen Grundsätzen wie die Regierungsvorlage ausgeht, jedoch die konkreten Bestimmungen einem einfachen Bundesgesetz vorbehält, wurde vom **Verfassungsausschuß des Nationalrates** ein Unterausschuß eingesetzt.

Dieser führte bei im wesentlichen bestehender politischer Übereinstimmung über die Notwendigkeit eines Datenschutzgesetzes Verhandlungen durch und hörte Experten an. Die Experten nahmen zur Regierungsvorlage positiv Stellung, regten aber einzelne Erweiterungen an.

Der Unterausschuß „Datenschutz" des Verfassungsausschusses des Nationalrates schloß am 24. Juni 1975 seine Arbeiten für die XIII. GP ab, ohne eine Beschlußfassung über die Regierungsvorlage und über den Initiativantrag der ÖVP herbeizuführen. In dieser Sitzung wurden die Ergebnisse des vom Unterausschuß eingesetzten Expertenausschusses zur Kenntnis genommen. Dabei ist insbesondere auf die Zusammenfassung des Protokolles des Expertenhearings vom 25. April 1975 zu verweisen, dessen Ergebnis nach Meinung des Unterausschusses für die weitere rechtspolitische Arbeit am Datenschutz ausschlaggebend sein soll:

a) Der Erweiterung des Geltungsbereiches eines Datenschutzgesetzes über die mit EDV geführten Datenbanken hinaus.
b) Strengere und differenziertere Bestimmungen für die Datenverarbeitung im privaten Bereich.
c) Datenschutz soll den Rang eines verfassungsgesetzlich gewährleisteten Rechtes in Präzisierung des Art. 8 EMRK erhalten, an dem einfache Gesetzesbestimmungen über die Datenweitergabe geprüft werden können (vgl. den Vorschlag unter 1.7.1).
d) Die Befugnisse der Datenschutzkommission sollen in Richtung auf eine auch präventive Kontrolle erweitert werden.

Entsprechend dieser Aussagen der Experten werden für den privaten Bereich Erhebungen mit Hilfe eines vom Präsidenten des Nationalrates an Interessenvertretungen und ähnliches gesandte Schreiben über bestehende Datenbanken durchgeführt sowie Professoren der Informatik um Stellungnahmen zu den Begriffsbestimmungen der Regierungsvorlage ersucht. Eine Auswertung der noch nicht vollständig eingelangten Antwort konnte noch nicht vorgenommen werden.

Ein mit dem Datenschutz am Rande zusammenhängendes Problem war ebenfalls Gegenstand der Verhandlungen im Unterausschuß: Das des **Zugriffsrechtes der Abgeordneten** der gesetzgebenden Körperschaften auf **Datenbanken der Verwaltung,** insbesondere der Bundesministerien. Der bestehende Informationsvorsprung der Verwaltung würde durch den Aufbau von Datenbanken vor allem seitens der Bundesministerien noch vergrößert. Den Abgeordneten steht bei gegebener Rechtslage nur ein mittelbares Kenntnisrecht über die in diesen Datenbanken enthaltenen Informationen zu, nämlich in Form der parlamentarischen Anfragen (Art. 52 B-VG). Nach einem Teil der Lehre findet allerdings dieses Anfragerecht seine Grenze bei Informationen, die der Amtsverschwiegenheit unterliegen. Allgemein wird davon auszugehen sein, daß sich das Interpellationsrecht nach Art. 52 B-VG und das Untersuchungsrecht nach Art. 53 B-VG auch auf die Kenntnisnahme von Daten aus Datenbanken erstreckt, da die Verfassung keine Unterscheidung nach der technischen Aufbewahrung der Informationen trifft und die Verwaltung auch nicht durch den Aufbau einer Datenbank oder den Einsatz einer EDV-Anlage die Kontrollrechte des Parlamentes umgehen kann. Inwieweit aber unabhängig von der Art der Daten den Abgeordneten ein direkter Zugriff auf Datenbanken der Verwaltung — das heißt, nicht im formellen Weg einer Anfrage nach der Geschäftsordnung des Nationalrates, sondern durch unmittelbaren (technischen) Zugriff ohne Dazwischentreten eines Organs der Verwaltung oder eines Mitgliedes der Bundesregierung — zustehen soll, bedarf wohl einer besonderen verfassungsgesetzlichen Regelung, die das grundsätzliche Verhältnis von Parlament und Regierung betrifft und weit über die Fragen des Datenschutzes hinausgeht, ganz abgesehen von den zu lösenden technischen Problemen und den notwendigen Bedienungskenntnissen der Abgeordneten oder ihrer Mitarbeiter.

In Österreich haben sich fast alle im Begutachtungsverfahren beteiligten Stellen zu einer auf dieses Problem bezugnehmenden Frage negativ geäußert, sodaß eine Aufnahme einer solchen Bestimmung in die Regierungsvorlage unterblieb.

Der österreichischen **Öffentlichkeit** ist in den letzten beiden Jahren die Forderung nach einem Datenschutz bewußt geworden. Es wurden wissenschaftliche Diskussionsveranstaltungen abgehalten (z. B. von der Österreichischen Juristenkommission, von der Österreichischen Gesellschaft für Politik, von der Arbeitsgemeinschaft für Datenverarbeitung) sowie rechtswissenschaftliche Arbeiten publiziert.

Des öfteren wird auch in Meldungen der Tagespresse auf mögliche Mißbräuche personenbezogener Daten hingewiesen, ohne daß aber bisher konkrete Fälle bewiesen worden sind. Die österreichische Öffentlichkeit ist sich der Notwendigkeit des Schutzes der Privatsphäre jedenfalls bewußt geworden.

Auch seitens der öffentlichen Verwaltung besteht das Bedürfnis nach einem Datenschutzgesetz, da damit die gegebene Rechtsunsicherheit beim Einsatz der modernen Datenverarbeitungstechniken, bei dem ja langfristig geplant werden muß, im Hinblick auf ein künftiges Datenschutzgesetz verringert würde.

Um dem Nationalrat die baldige Wiederaufnahme der Behandlung eines Datenschutzgesetzes zu ermöglichen und um der Regierungserklärung vom 5. November 1975 gerecht zu werden, wird den gesetzgebenden Körperschaften erneut die Regierungsvorlage eines Datenschutzgesetzes übermittelt. Diese Regierungsvorlage weist gegenüber der vom Dezember 1974 nur geringfügigste textliche Änderungen auf, enthält aber in den Erläuterungen Hinweise und Anregungen zur bisherigen und weiteren legislativen Arbeit im Nationalrat.

1.7 Die Grundsätze der Regierungsvorlage

1.7.1 Der vorliegende Entwurf verzichtet auf einen verfassungsgesetzlichen Schutz der in Datenbanken gespeicherten Daten. Der **Schutz des Privatlebens** ist ein ganz allgemeines Problem, das nicht isoliert hinsichtlich der Datenverarbeitung behandelt werden kann. Dieses Problem wird daher auch im Zuge der ohnehin geplanten Neukodifikation der Grundrechte zu behandeln sein. Im übrigen ist das Privatleben bereits jetzt gegen Eingriffe der öffentlichen Hand durch Art. 8 der Europäischen Menschenrechtskonvention geschützt. Der durch diese Bestimmung der Europäischen Menschenrechtskonvention gewährleistete Schutz wird zumindest im gegenwärtigen Zeitpunkt nicht zuletzt deshalb als ausreichend angesehen werden können, weil Österreich sowohl das Individualbeschwerderecht als auch die obligatorische Gerichtsbarkeit des Europäischen Gerichtshofes für Menschenrechte durch Erklärung gemäß Art. 25 und Art. 46 der Europäischen Menschenrechtskonvention anerkannt hat. Um aber einerseits verschiedenen Anregungen der Begutachtungsverfahren Rechnung zu tragen und um andererseits einen Hinweis für die Begegnung der Gefahr für einen effektiven Datenschutz zu geben, die darin liegt, daß dem Datenschutzgesetz als einfachem Bundesgesetz durch spätere Gesetze derogiert werden kann bzw. daß die Bestimmungen des Datenschutzgesetzes, von denen eine Ausnahme möglich ist (z. B. § 7), durch eine große Zahl von Ausnahmen faktisch obsolet werden, wird ein Diskussionsentwurf für eine Verfassungsbestimmung vorgelegt, mit der das Staatsgrundgesetz über die allgemeinen Rechte der Staatsbürger 1967 (in der Fassung des Bundesverfassungsgesetzes BGBl. Nr. 8/1974) durch einen Art. 10 b ergänzt werden könnte:

„(1) Personenbezogene Daten sind geheimzuhalten, soweit dies Interessen der betroffenen Person oder öffentliche Interessen erfordern.

(2) Es dürfen nur solche Daten erhoben werden und verarbeitet werden, die zur Erreichung eines erlaubten Zweckes unbedingt erforderlich sind.

(3) Jedermann hat grundsätzlich das Recht zu wissen, wer Daten über ihn erhebt und verarbeitet, welcher Art diese Daten sind, von wo diese Daten stammen, wozu sie verwendet und an wen sie weitergegeben werden, es sei denn, das Interesse einer betroffenen Person oder das öffentliche Interesse stehen dem entgegen.

(4) Jedermann hat das Recht, die Berichtigung der ihn betroffenen Daten und die Löschung unzulässigerweise erhobener und verarbeiteter Daten zu verlangen.

(5) Die Daten sind so zu verarbeiten, daß sie nicht durch Unbefugte eingesehen, verändert, abgerufen oder vernichtet werden können."

Eine solche oder ähnliche programmatische Bestimmung wäre als Ergänzung zu Art. 8 EMRK zu verstehen. Hinsichtlich der in ihr erwähnten Termini der Datenverarbeitung wird auf die Begriffsbestimmungen in und die Erläuterungen zu § 2 der Regierungsvorlage verwiesen. Die Grundsatzbestimmung enthält mit Rücksicht darauf, daß eine Interessensabwägung für sämtliche Lebensbereiche nicht generell abstrakt vorgenommen werden kann, letztlich eine Fülle von Gesetzesvorbehalten („erlaubte Weise", „erlaubter Zweck", „unzulässigerweise", „unbefugte"). Die einfachgesetzlichen Regelungen können daher aus rechtspolitischen Gründen für die jeweiligen konkreten Lebensbereiche in nicht diskriminierender Weise Interessensabwägungen durchführen. Solche gesetzlichen Regelungen müßten jedoch so beschaffen sein, daß sie das grundsätzliche Ziel der Verfassungsbestimmung, den Schutz der Privatsphäre des Einzelnen (physische oder juristische Person) zu gewährleisten, nicht hinfällig machen.

Für die Datenbanken der öffentlichen Hand (vgl. § 3, § 4 der Regierungsvorlage) würden die Bestimmungen der Regierungsvorlage dem Diskussionsentwurf einer Ergänzung des Staatsgrundgesetzes entsprechen, sodaß eine Verabschiedung auch des Art. 10 b StGG möglich wäre. Da sich die Regierungsvorlage aber nur auf mit EDV geführten Datenbanken beschränkt, könnten sich für die mit konventionellen Mitteln vorgenommenen Datenerhebungen und Datenverarbeitungen die Notwendigkeit eines gesonderten Ausführungsgesetzes zu Art. 10 b StGG ergeben.

Daß die Regierungsvorlage hinsichtlich der Datenbanken Privater keinen dem Grundgedanken des Diskussionsentwurfes des Art. 10 b entsprechend weitreichenden Schutz vor Datenverarbeitung enthält, ist im Lichte der Problematik der sogenannten Drittwirkung von Grundrechten zu sehen, wobei der Verfassungsgerichtshof im Erkenntnis G 8/74 vom 11. Oktober 1974 (zu § 94 Abs. 1 Z 1 StGB 1974) sich gegen die Drittwirkung von Grundrechten ausgesprochen hat.

Die Justizibialität von Verfassungsgrundsätzen, wie sie der vorstehende Diskussionsentwurf enthält, im Verhältnis zwischen Privaten stellt ein in der österreichischen Rechtsordung noch ungelöstes Problem dar und bildet den Gegenstand auch von Diskussionen im Rahmen des Grundrechtskollegiums. Es wird dem einfachen Gesetzgeber obliegen, durch entsprechende zivilrechtliche, strafrechtliche und sonstige Bestimmungen die Wirksamkeit dieser Grundsätze zu gewährleisten. Dies geschieht zum Teil durch die Bestimmungen der Regierungsvorlage (vgl. § 24 bis § 29), zum Teil durch bereits bestehende gesetzliche Vorschriften (z. B. § 69 Abs. 2 Gewerbeordnung 1973, § 121, § 122, § 152 StGB 1974, § 47 KWG; vgl. dazu G. Stadler ÖZW 1974, a. a. O.).

Art. 10 b StGG wäre im Lichte des Grundsatzes der österreichischen Verfassungsrechtsordnung zu sehen, wonach gemäß Art. 18 B-VG das staatliche Handeln stets einer entsprechenden einfachgesetzlichen Grundlage bedarf, privates Handeln hingegen so lange erlaubt ist, als nicht besondere gesetzliche Vorschriften die Handlungsfreiheit des Einzelnen einschränken.

Die durch den Diskussionsentwurf statuierten Grundsätze decken sich zum Teil mit bestehenden Grundsätzen der österreichischen Verfassungsordnung, die ebenfalls demselben Ziel, dem Schutz der Freiheitssphäre des Einzelnen dienen, wie Art. 18 B-VG und Art. 20 Abs. 2 B-VG sowie Art. 8 EMRK.

1.7.2 Anwendungsbereiche des Datenschutzgesetzes sollen nunmehr alle Datenbanken des öffentlichen Bereiches sein, die mit EDV oder vergleichbaren Techniken geführt werden. Was unter öffentlichem Bereich zu verstehen ist, ergibt sich aus § 3 und § 4. Vom Geltungsbereich mußten aus verfassungsrechtlichen Gründen grundsätzlich ausgenommen werden die Datenverarbeitung (in Datenbanken im Sinne der Regierungsvorlage) von oder im Auftrag von Organen der Gesetzgebung (§ 3 Abs. 2), was gegenwärtig in Österreich noch nicht geschieht. Darüber hinaus wurde auch die Datenverarbeitung in Datenbanken in den Geltungsbereich einbezogen, die in Form eines privatrechtlichen Vertrages von Rechtsträgern des öffentlichen Bereiches in Auftrag gegeben wird (§ 14).

Der Entwurf enthält auch eine grundsätzliche Einbeziehung von Datenbanken Privater, wobei die Bundesregierung vom Grundgedanken einer verwaltungsökonomischen Gestaltung ausging und die bereits bestehenden Aufsichtsbehörden auch mit der Aufgabe der Aufsicht über EDV-Datenbanken betrauen will (§ 26). Daneben wurden in Ergänzung zum 5. Abschnitt des besonderen Teiles des StGB 1974 Strafbestimmungen vorgesehen, die auch auf den Täter anzuwenden sind, der personenbezogene Daten in oder aus privaten Datenbanken mißbraucht (§ 27 bis § 29). Es wurde bei den privaten Datenbanken keine Unterscheidung vorgenommen, ob die Datenbank im Rahmen des Unternehmenszwecks (z. B. Kreditauskunftei) oder im Rahmen eines innerbetrieblichen Informationssystems (z. B. Personalinformationssystem) geführt werden. Um eine Umgehung des Datenschutzgesetzes durch im Ausland gelegene Datenverarbeitungsanlagen zu verhindern (die Mehrzahl der privaten Datenbanken mit sensiblen Datenbanken über Staatsbürger der USA befindet sich in Kanada, um den strengeren Datenschutzbestimmungen der USA zu entgehen), wird vorgesehen, daß ausländische Datenverarbeitungsanlagen von Unternehmen, die ihren Sitz in Österreich haben, nur unter denselben Bedingungen personenbezogene Daten verarbeiten dürfen, unter denen sie dies in Österreich dürften.

1.7.3 Die Regierungsvorlage enthält eine **Verfassungsbestimmung** zugunsten des Bundes, um sicherzustellen, daß alle EDV-Datenbanken (privater und öffentlicher Bereich) denselben gesetzlichen Bestimmungen unterliegen. Das Schutzbedürfnis personenbezogener Daten — die für sich je nach dem Kompetenztatbestand zu beurteilen sein würden, für den sie erhoben worden sind — ist unabhängig von ihrer Zuordnung zu einem Kompetenzbereich und unabhängig von ihrer Verarbeitung in einer Datenbank einer Bundes- oder einer Landesdienststelle. Aus diesen rechtspolitisch gerechtfertigten Gründen wurde eine Kompetenzänderung nur hinsichtlich der Zuständigkeit in der Gesetzgebung zugunsten des Bundes vorgesehen. Der Schutz der Daten und der Grundrechtssphäre soll von der kompetenzrechtlichen Zuordnung der Datenbank zunächst unabhängig sein, allerdings obliegt die Vollziehung des Datenschutzgesetzes den Ländern, soweit es sich um Datenbanken von Rechtsträgern handelt, deren Einrichtung in der Vollziehung Landessache ist (§ 4).

1.7.4 Entgegen dem Entwurf vom 16. Mai 1974 beschränkt sich die Regierungsvorlage auf mit **EDV oder vergleichbaren Techniken geführte Datenbanken,** da die während des Begutachtungsverfahrens durchgeführte Erhebung über Datenbanken zeigte, daß die gewählte numerische Abgrenzung (vgl. oben) im Hinblick auf die Möglichkeit der Aufspaltung von Datenbanken in einzelne Datenbestände sehr problematisch und umgehbar wäre. Die Mehrzahl der konventionell (manuell) geführten Datensammlungen besteht bereits seit langer Zeit, ohne daß nun ein besonderes Rechtschutzbedürfnis aufgetaucht wäre. Durch den Einsatz der EDV in Datensammlungen entsteht aber eine neue Qualität der Informationsmöglichkeit und damit der Gefährdung der Privatsphäre, insbesondere durch die große Speichermöglichkeit, die hohe Verarbeitungs-

geschwindigkeit, die Kombinationsmöglichkeiten, die dezentrale Abfrage zentraler Speicher u. a. Diese technischen Gegebenheiten lassen eine Einschränkung des Datenbankbegriffes (§ 2 Z 10) auf mit Hilfe der EDV oder ähnlicher Mittel geführte Datensammlungen sachlich gerechtfertigt erscheinen; an die Umstellung einer Datenbank auf EDV, die meist eindeutig feststellbar ist, würde sich bei bereits bestehenden Datensammlungen die Anwendung des Datenschutzgesetzes knüpfen.

1.7.5 Das Gesetz soll nicht nur auf künftige Datenbanken Anwendung finden, sondern auch auf bestehende. Daß bestehenden gesetzlichen Geheimhaltungsverpflichtungen bzw. Auskunftsberechtigungen nicht derogiert werden soll, ergibt sich aus den **Subsidiaritätsklauseln** des § 7. Auch im übrigen verweist das Datenschutzgesetz grundsätzlich auf die gesetzlichen Bestimmungen, die die Grundlagen für die Datenerhebung und -verarbeitung abgeben und auch deren Beschränkungen normieren bzw. normieren sollen (§ 6, § 8). Das Datenschutzgesetz soll weder ohne gesetzliche Grundlagen bestehende Datenbanken mit personenbezogenen Daten legalisieren noch allein die Grundlage für derartige Datenbanken geben, aber es soll sichern, daß für alle Datenbanken, die personenbezogene Daten enthalten, einheitliche, dem Schutz der Privatsphäre dienende Vorschriften und Rechtsbehelfe bestehen.

1.7.6 Im Sinne der oben angeführten, aus der Rechtsvergleichung gewonnenen Prinzipien des Datenschutzrechtes soll auch dieses Gesetz die Privatsphäre gegenüber dem Mißbrauch öffentlicher Datenbanken durch eine **Mehrzahl aufeinander abgestimmter Vorkehrungen** schützen:

Die Verarbeitung personenbezogener Daten soll nur auf Grund von Gesetzen und nur in Datenbanken möglich sein, für die durch eine in Form einer Verordnung erlassene Betriebsordnung sichergestellt ist, daß den Gedanken des Datenschutzes und der Datensicherheit Rechnung getragen wird.

Die Weitergabe von dem Amtsgeheimnis unterliegenden personenbezogenen Daten soll nur zulässig sein auf Grund ausdrücklicher gesetzlicher Bestimmung oder mit schriftlicher Zustimmung des Betroffenen, bzw. bei Anonymisierung der Daten, es sei denn, es handelt sich dabei um Daten, deren Geheimhaltung nicht ausschließlich im Interesse der Betroffenen geboten ist. Eine Verknüpfung personenbezogener Daten, die für verschiedene Datenbanken gesammelt wurden, bedürfte einer ausdrücklichen gesetzlichen Ermächtigung bzw. dürfen die Daten dem spezifischen Zweck, zu dem sie erhoben wurden, nicht entfremdet werden.

Dem Betroffenen steht ein Einsichtsrecht in die ihn betreffenden Daten zu und ein Berichtigungsanspruch.

Alle Datenbanken, die personenbezogene Daten verarbeiten, sind jährlich in einem Kundmachungsorgan bekanntzugeben mit der Angabe der Art der in ihnen gespeicherten Daten und des Kreises der Betroffenen.

Der organisatorische Schutz soll durch je eine nach Art. 133 Z. 4 B-VG eingerichtete Datenschutzkommission (Bundes-Datenschutzkommission, Landes-Datenschutzkommissionen) erreicht werden, die gegen Beschwerden wegen der Behauptung der Verletzung von Bestimmungen des Datenschutzgesetzes entscheiden soll und insbesondere Berichtigungsaufträge an die Datenbanken erteilen kann.

Der Entwurf sieht weiters gerichtliche Strafbestimmungen vor.

1.8 Aufwand

Über die sich bei Anwendung dieses Gesetzes ergebenden Kosten an Personal- und Sachaufwand können gegenwärtig keine konkreten Angaben gemacht werden, da dies wesentlich von der Zahl und vom Umfang der unter dieses Gesetz fallenden Datenbanken abhängen wird und sich diese Zahl mit dem zunehmenden Einsatz der EDV in der Verwaltung erhöht. Ausführliche Untersuchungen über die Kosten von Datenschutz- und Datensicherungsmaßnahmen sind unbekannt und würden auch nur vage Schlüsse auf den mit diesem Bundesgesetz zu erwartenden Aufwand zulassen, da die Kosten wesentlich von der konkreten rechtlichen und faktischen Gestaltung des Datenschutzes und insbesondere der Datensicherheit abhängen. Verschiedene Erfahrungen, so nach dem schwedischen Datenschutzgesetz und in der deutschen Privatwirtschaft zeigen, daß sich die Gesamtkosten (Personal, Gebäude, Maschinen und Programme) für die Datenverarbeitung bei einem effektiven Datenschutz um 7% bis 10% erhöhen. Die Erhöhung ist vor allem durch Vorschriften über die Datensicherheit bedingt (erhöhter Gebäudeschutz, Duplizierung von Datenbeständen, Ausarbeitung bzw. Miete von Software, die Datenschutzprogramme enthält) und schlägt sich daher sowohl bei den Raumkosten als auch bei den Kosten für Hardware und für Software nieder. Allenfalls werden noch Versicherungsprämien für die Haftungsdeckung bei Datenverfälschung u. ä. als Kostenfaktor zu veranschlagen sein. Die Personalkosten stellen demgegenüber einen wesentlich geringeren Erhöhungsfaktor dar.

Wenn man für den Bundesbereich von 799 Millionen Schilling an EDV-Gesamtkosten für 1974 ausgeht (1976: 1068 Millionen Schil-

ling; vgl. EDV-Bericht und Prognose der Bundesregierung 1973, S. 43, III-123 d. Blg. Stenogr. Prot. NR, XIII. GP), und berücksichtigt, daß 20% dieser Beträge im wissenschaftlich-akademischen Bereich anfallen, wo kaum Datenbanken mit personenbezogenen Daten vorhanden sind, und weiters berücksichtigt, daß auch in der Hoheitsverwaltung und in den Betrieben des Bundes nur ein Teil der EDV-Kosten auf Datenbanken im Sinne der Regierungsvorlage entfiele, so könnte 1977 bei Preisen von 1974 eine Summe von 70 Millionen Schilling für Datensicherung eine annähernde Schätzung beinhalten. In der Folge wird sich diese Summe jährlich in Relation zu den Budgetaufwendungen des Bundes für EDV erhöhen bzw. ermäßigen (erhöhter Anfangsaufwand für Erstprogrammierungen).

Für die nicht vom Bundesbudget erfaßten Rechtsträger (Sozialversicherungen, Länder, Gemeinden, Private u. a.) kann nur die oben erwähnte prozentuelle Erhöhung prognostiziert werden.

Die Kostenerhöhung wird zudem von der Art der verarbeiteten Daten (da die Datenbank-Verordnung gemäß § 9 Abs. 1 je nach der Sensibilität der Daten zu gestalten ist und ein Mehr an Sicherheit ein Mehr an Kosten verursacht) und vom Umfang der bereits bisher getroffenen Sicherungsmaßnahmen abhängen.

Während das Berichtigungsrecht der Betroffenen kostenmäßig kaum ins Gewicht fallen wird, kann das Auskunftsrecht bei häufiger Beanspruchung eine hinsichtlich Hardware-Ausstattung und Maschinenzeit nicht unbeträchtliche Erhöhung der EDV-Kosten bringen, wobei aber eine wenigstens teilweise Deckung durch die Möglichkeit der Einhebung einer Verwaltungsabgabe (§ 10 Abs. 3) vorgesehen werden kann.

Die Mitglieder der Bundes-Datenschutzkommission sollen nebenberuflich tätig sein, sodaß ein erhöhter Bedarf an Dienstposten nur infolge eines allenfalls notwendigen Sekretariatspersonals entstehen wird, wobei dies ebenso wie die Höhe der Entschädigung für die Mitglieder der Datenschutzkommission von der Zahl der Beschwerden und der amtswegig eingeleiteten Verfahren abhängen wird, worüber gegenwärtig keine Aussage getroffen werden kann.

1.9 Anbetracht der vom Datenschutzgesetz geforderten konkreten gesetzlichen Bindung des Datenverkehrs an gesetzlichen Bestimmungen könnte es — wie sich aus der im Begutachtungsverfahren durchgeführten Erhebung über bestehende oder projektierte Datenbanken ergibt — notwendig sein, dem Nationalrat **weitere Gesetzentwürfe** über die Voraussetzung der Erhebung und Verarbeitung personenbezogener Daten in einzelnen Datenbanken vorzulegen.

2. Zu den einzelnen Bestimmungen

Zum Titel: Der Titel bezieht sich nicht nur auf den Schutz personenbezogener Daten in EDV-Datenbanken, da das Gesetz in einzelnen Bestimmungen personenbezogene Daten auch dann schützt, wenn diese nicht, noch nicht oder nicht mehr, in der Datenbank enthalten sind. (Z. B. Erhebung von Daten; die Strafbestimmungen wirken auch gegen den, der im Zeitpunkt der Tat nicht mehr bei einer Datenbank beschäftigt ist.) Neben einem Kurztitel bildet auch eine Abkürzung aus schreibökonomischen Gründen einen Bestandteil des Titels.

Zur Systematik:

Die Regierungsvorlage ist in 7 Abschnitte gegliedert:

— allgemeine Bestimmungen (Zuständigkeit, Begriffsbestimmungen, Anwendungsbereich)

— Verarbeitung personenbezogener Daten (Zulässigkeit der Erhebung und Verarbeitung von Daten, Datenbank-Verordnung, Rechte der Betroffenen auf Auskunft und auf Berichtigung, Publikation einer Liste der Datenbanken)

— vertragliche Inanspruchnahme von Datenverarbeitung durch die in § 3 und § 4 genannten Rechtsträger (Voraussetzung der Datenverarbeitung im Auftrag der öffentlichen Hand)

— Bundes-Datenschutzkommission (Einrichtung, Zusammensetzung und Verfahren, Bericht an die Bundesregierung; die Bestimmungen gelten entsprechend für die Datenschutzkommissionen der Länder)

— private Datenbanken (Aufsicht, Beschränkung von Datenverarbeitung im Ausland)

— Strafbestimmungen

— Schlußbestimmungen (Inkrafttreten, eigener Wirkungsbereich der Gemeinde, Vollziehung).

Zu § 1:

In dieser Verfassungsbestimmung soll für den Bund die Zuständigkeit zur Gesetzgebung hinsichtlich des Schutzes personenbezogener Daten, soweit diese mit Hilfe der EDV verarbeitet werden, festgelegt werden. Dem bundesstaatlichen Gedanken wird dadurch Rechnung getragen, daß die Vollziehung solcher Gesetze den Ländern zusteht, wenn die Daten von oder im Auftrage des Landes oder im Auftrage einer juristischen Person, deren Einrichtung in der Vollziehung in die Zuständigkeit der Länder fällt, verarbeitet werden. Für die Erhebung und Verarbeitung von Daten mit konventionellen Mitteln werden die Kompetenztatbestände des B-VG in der geltenden Fassung heranzuziehen sein (vgl. oben). Wird aber die Erhebung mit dem Ziel vorgenommen, die erhobenen Daten in EDV-Datenbanken zu verarbeiten (vgl. § 6), so wird auch darauf § 1 DSG anzuwenden sein, da der Schutz per-

sonenbezogener Daten nicht bei der Verarbeitung im technischen Sinn, sondern auch bereits bei der Erhebung (im Sinne des § 2 Z. 4) einzusetzen hat; jedenfalls findet aber das DSG auch auf Daten Anwendung, wenn diese zwar für eine manuelle Datensammlung erhoben wurden, aber dann auf eine Datenbank im Sinne des § 2 Z. 10 umgestellt werden.

Zweifelsfälle über das Vorliegen „elektronischer Datenverarbeitung" sind nicht ausgeschlossen, doch ist dieser Begriff in der Informationswissenschaft bereits derart reichhaltig behandelt, daß es gerechtfertigt erscheint, ihn als terminus legalis zu verwenden. Als Beispiel für eine Definition sei die aus dem Lexikon für Datenverarbeitung 1969, S. 129, wiedergegeben: „Elektronische Datenverarbeitung ist die programmgesteuerte Speicherung und die Verarbeitung von Informationen mit Hilfe elektronischer Hilfsmittel, die nur Beziehungen verarbeiten können, die durch eine endliche Zahl logisch-mathematischer Formeln ausgedrückt werden können." Da die Entwicklung der EDV-Technologie gegenwärtig nicht abzusehen ist und ein Übergang von elektronischen Techniken auf andere (z. B. Laser-Technik, Ausnützung optischer Prozesse) möglich scheint, wurde die Einfügung „oder vergleichbarer Techniken" gemacht, wobei sich „vergleichbar" in Relation zu den technischen Möglichkeiten bzw. der Effizienz im Hinblick auf die Menge der gespeicherten Daten, auf die Schnelligkeit der Datenverarbeitung, auf die Datenfernverarbeitung und auf den Umfang der Datenkombination beziehen soll.

Der Begriff des „Auftrages" im 2. Satz ist hier nicht auf den privatrechtlichen Auftrag oder Vertrag beschränkt (vgl. § 14), sondern kann sich auch auf ein öffentlich-rechtliches Verhältnis zwischen Behörden beziehen, wobei die organisatorische Zurechnung der beauftragenden Stellen den Ausschlag für die Zurechnung der Vollziehung des DSG (vgl. § 4) gibt.

Der Satz 3 soll es dem Bundesgesetzgeber, sofern er für die Regelung der Verwaltungsmaterie zuständig ist, ermöglichen vorzusehen, daß die Durchführungsverordnungen zum DSG (z. B. § 9) vom zuständigen Bundesminister auch für jene Datenbanken erlassen werden, die von den Ländern oder Gemeinden geführt werden (z. B. Datenbanken über Meldedaten), um hier notwendige bundeseinheitliche Durchführungen zu sichern.

Zu § 2:

§ 2 enthält die für die Feststellung des Anwendungsbereiches und für die Vollziehung des Gesetzes notwendigen spezifischen Begriffsbestimmungen. Auch bei diesen Begriffsbestimmungen wurde auf die internationalen Erfahrungen zurückgegriffen, wobei nochmals darauf hinzuweisen ist, daß es für die Begriffe „personsbezogene Daten" (personal information) u. ä. und „Datenbank" keine allgemein gültigen Begriffsbestimmungen gibt und eine Definition von der Wissenschaft zum Teil überhaupt abgelehnt wird (vgl. zuletzt S. Simitis, Datenschutz — Notwendigkeit und Voraussetzungen einer gesetzlichen Regelung, in: Datenverarbeitung im Recht, 1973/2—3, 148), was aber eine legistisch nicht durchzuführende Lösung darstellt.

Zu Z. 1:

Der Begriff der **„personsbezogenen Daten"** wird vom Entwurf bewußt sehr weit gefaßt, da davon ausgegangen wird, daß eigentlich jedes individuell-konkrete Datum und ein Teil der aggregierten Daten — nämlich die, die sich ohne große Schwierigkeiten wieder auf Angaben über Einzelpersonen zurückführen lassen — allein oder im Verbund mit anderen Daten letztlich Aussagen über Menschen oder über juristische Personen enthält und eine negative Abgrenzung zu die Privatsphäre nicht berührenden Daten nicht möglich ist. Dies wird klar an einem Beispiel von Daten über die Bonität eines Grundstückes, die zunächst objektbezogen sind, aber in Verbindung etwa mit einem Auszug aus dem Grundbuch sehr wohl Bereiche der Privatsphäre, nämlich des Vermögensstandes berühren. „Aussagen" soll weiters zeigen, daß nicht nur Fakten, sondern auch bloße Hinweise und Vermutungen sowie rechtliche Zuordnungen unter den Begriff der personenbezogenen Daten fallen. Es sind darunter sowohl Angaben über persönliche wie über wirtschaftliche Bereiche (z. B. Kontonummer, Autonummer, Automarke) zu verstehen. Wirtschaftlich ist nicht im Sinne von erwerbswirtschaftlich gemeint, sondern umfaßt etwa auch den caritativen Bereich, den Bereich der Freizeit.

Personenkennzeichen, wie sie § 31 Abs. 3 Z. 14 ASVG (Sozialversicherungsnummer) und der Entwurf eines Bevölkerungsevidenzgesetzes (GZ. 11016/18-SL/IV/74 des Bundesministeriums für Inneres vom 18. März 1974) enthalten, sollen auch dann unter den Schutz des DSG fallen, wenn in ihnen nicht personenbezogene Aussagen (z. B. Geburtsdatum) verschlüsselt sind. Die Einbeziehung in das Datenschutzgesetz ist aus der wesentlichen Erleichterung, die Personenkennzeichen — d. s. Zeichenkombinationen (numerische und/oder alphanumerische Zeichen), die nach bestimmten Regeln für eindeutig bestimmte physische oder juristische Personen vergeben und als Ordnungskriterium für Informationskategorien (Datensätze) herangezogen werden — für die Verknüpfung personenbezogener Daten bringen, begründet.

Das Gesetz soll Daten über physische und über juristische Personen (einschließlich der Personen

des öffentlichen Rechts) sowie über handelsrechtliche Personengesellschaften (OHG, KG) schützen. Der Schutz juristischer Personen (und handelsrechtlicher Personengesellschaften, die in der österreichischen Rechtsordnung zum Großteil juristischen Personen des Privatrechtes gleichgestellt sind) wurde in der internationalen Datenschutzdiskussion überwiegend abgelehnt (vgl. die unter 1.2 übersetzte Resolution des Ministerkomitees des Europarates, § 3 Abs. 1 des Entwurfes der deutschen Bundesregierung, § 1-1 des Entwurfes für ein Norwegisches Datenschutzgesetz; Simitis a. a. O.; § 1 Abs. 4 des Alternativentwurfes für ein deutsches Bundesdatenschutz-Rahmengesetz von A. Podlech bezieht dagegen Personengruppen ein, vgl. A. Podlech, Datenschutz im Bereich der öffentlichen Verwaltung, 1973), doch scheint ein Gruppenschutz, bzw. ein Schutz von Personenmehrheiten (z. B. Verein) deswegen gerechtfertigt, weil sich einerseits die Mehrheit der Informationen über eine juristische Person auch wiederum auf Informationen über eine physische Person zurückführen läßt, und die Datenverarbeitung andererseits eine Bedrohung auch von Kollektivinteressen darstellt.

Die Regierungsvorlage verwendet konsequent den Begriff „Daten" und versteht darunter mit der herkömmlichen Definition Zeichen oder Zeichenketten, die in einem Entscheidungsprozeß relevante Bedeutung für den Entscheider haben und deren semantische Bedeutung mit Hilfe von Interpretationsregeln, die dem Entscheider bekannt sind, zu vollständigen Aussagen ergänzt werden kann (vgl. W. Killian — K. Lenk — W. Steinmüller, Datenschutz, 1973, 210 ff; weiters DIN 44300, Nr. 19). Datenschutz im Sinne dieses Gesetzes betrifft somit Daten, aus denen Informationen, das sind die die Verbindung zwischen Sachverhalten auf der einen Seite und dem Entscheidungsprozeß auf der anderen Seite herstellenden Elemente, gewonnen werden können. Grundsätzlich aus dem Datenschutz im Sinne dieser Vorlage ausgeklammert bleibt somit der Schutz der Programme, auf den allenfalls bei den Datenbank-Verordnungen Rücksicht zu nehmen sein wird.

Zu Z. 2:

Als **Betroffene** werden in der Folge die physischen oder juristischen Personen sowie handelsrechtliche Personengesellschaften bezeichnet, über die personenbezogene Daten erhoben oder verarbeitet werden und denen auf Grund dieser Erhebung oder Verarbeitung eine besondere Rechtsstellung im Sinne dieses Gesetzes zukommt. Den Betroffenen steht etwa das Recht auf Auskunft (§ 10), auf Berichtigung (§ 11), auf Erhebung einer Beschwerde vor der Datenschutzkommission (§ 20) zu.

Zu Z. 3:

Der Begriff der **Datenverarbeitung** umfaßt die in den Z. 5 bis 9 umschriebenen Tätigkeiten mit Daten, und zwar unabhängig von der Technik, mit deren Hilfe diese Tätigkeiten ausgeführt werden. Der Anwendungsbereich des Datenschutzgesetzes beinhaltet also noch nicht das Sammeln von Daten (vgl. aber Z. 4), wohl aber deren Aufnahme in die Datenbank, deren interne Manipulierung und ihre Ausgabe.

Zu Z. 4:

Eine Einbeziehung der Datenerhebung unter die Schutzbestimmungen des Datenschutzgesetzes scheint insofern gerechtfertigt, als diese Erhebung unter Mitwirkung des Betroffenen erfolgt und insoweit die Daten zum Zwecke einer Speicherung in einer Datenbank erhoben werden (§ 6). Die Abstellung auf die Mitwirkung wurde gewählt, weil diese meist durch gesetzliche Bestimmungen erzwungen werden kann (vgl. z. B. § 8 des Bundesstatistikgesetzes 1965) und hier ein erhöhter Rechtsschutz gegeben werden soll. Auch Daten, die ohne Mitwirkung des Betroffenen ermittelt wurden, unterliegen dem DSG. Das Vorliegen einer Erhebung im Sinne des § 2 ist weiters bedeutsam für die Beweislast bei einem Berichtigungsanspruch (§ 11 Abs. 2).

Zu Z. 5:

Der Begriff der **Speicherung** umfaßt das physische Erfassen der Daten auf einem Datenträger (das Schreiben der Karteikarten, das Ablochen, die Aufnahme auf Lochstreifen und auf Magnetbandkassetten, das EDV-unterstützte Beleglesen u. ä.). Voraussetzung ist, daß die Datenerfassung mit der Intention erfolgt, die Datenträger in einer Datenbank im Sinne des Gesetzes zu verwenden.

Zu Z. 6:

Das **Verändern** soll das inhaltliche Umgestalten von Daten umfassen; also nicht deren Transformierung auf andere Datenträger, wohl aber das Ändern der Daten selbst (z. B. Fortschreiben von Personaldaten).

Zu Z. 7:

Der Begriff der Verknüpfung beinhaltet zwei Komplexe: es werden für eine Datenbank erhobene oder in verschiedenen Datenbanken gespeicherte personenbezogene Daten in einer einzigen Datenbank verknüpft, sodaß aus einer Mehrheit getrennter Datensätze ein einziger entsteht, daß somit die Information für den Benützer nur einer der Datenbanken erweitert wird. Die Verknüpfung ist den Bedingungen des Gesetzes unterworfen, wenn sie vorübergehend (z. B. die konkrete Abfrage über personenbezogene Daten

aus zwei Datenbanken, die in der teleprocessing-Technik verbunden sind) oder wenn sie dauernd (mehrere bisher getrennte Datenbanken werden in einer EDV-Anlage vereinigt) erfolgt. Sind von einem Terminal Daten aus mehreren Datenbanken abrufbar, müßten für jede dieser Zugriffsmöglichkeiten die Bedingungen des § 7 zutreffen, sofern eine Weitergabe vorliegt. Unter „Verknüpfung" wird nicht die abstrakte dauernde technische Verbindung zwischen zwei Computern verstanden (Verbundsystem), die allerdings für unter dieses Gesetz fallende Datenbanken besonderen Sicherungsvorschriften unterliegen müßte (Datenbank-Verordnung, § 9).

Zu Z. 8:

Der Begriff der **Weitergabe** umfaßt die Ausgabe (in verschlüsselter Form oder im Klartext) von Daten an Empfänger, die außerhalb der die Datenbank führenden (d. h. in der eigenen Organisation oder im Auftrag geführt) Einrichtung stehen. Es fällt darunter daher auch die Weitergabe an über- oder untergeordnete Behörden.

Zu Z. 9:

Unter **löschen** wird die Verstümmelung oder Vernichtung von Daten verstanden.

Zu Z. 10:

Auf den Begriff der **Datenbank** wurde bereits eingangs hingewiesen (siehe 1.7.2). Kriterium für das Vorhandensein einer Datenbank im Sinne dieses Gesetzes ist zunächst die Ordnung einer Sammlung von personenbezogenen Daten nach einem oder mehreren festgelegten Merkmalen, d. h. die einzelnen Daten müssen kategorisiert sein (z. B. Reihung einer Personaldatei nach Zunamen, nach Geburtsdatum, nach Vorrückungsstichtag u. ä.). Die Kategorisierung der in einem Datensatz enthaltenen Informationen muß es ermöglichen, diese Daten nach (einem oder mehreren) anderen Merkmalen zu ordnen (z. B. Ordnung nach dem Tag des Eintrittes in den Dienst, nach der Dienststelle). Diese Möglichkeit wird in der Regel im Zeitpunkt der Speicherung bereits vorgesehen sein (daher wird etwa der Katalog einer Bibliothek in der Regel nicht unter Kriterien des Gesetzes fallen, auch wenn dieser mit EDV geführt würde). Ist eine EDV-Datenbank durch ihren Aufbau bereits mehrdimensional geordnet (z. B. mehrere files), so sind damit bereits die Kriterien der Z. 10 gegeben.

Über die Einschränkung des Gesetzes auf mit EDV geführte Datenbanken und über die der Regierungsvorlage zugrunde gelegte Begriffsbestimmung von „EDV" vgl. oben 1.7.4 sowie zu § 1. Eine derartige Abgrenzung gegenüber mit herkömmlichen Mitteln geführten Datensammlungen erscheint auch anbetracht des Schutzobjektes Persönlichkeitssphäre sachlich gerechtfertigt; das DSG wird aber auch schon anzuwenden sein, wenn auch nur eine der in Z. 3 zusammengefaßten Tätigkeiten der „Verarbeitung" mit EDV durchgeführt wird.

Durch den letzten Halbsatz der Z. 10 soll klargestellt werden, daß zur Datenbank nicht nur die Daten als Informationsquelle gehören, sondern auch die technischen Einrichtungen, auf denen die Daten gespeichert sind, und mit denen sie sonst verarbeitet werden. Ein derartiger Begriffsumfang ist insbesondere wegen der Bestimmungen des § 9 und des § 29 notwendig, um auch die Datenträger, die von der EDV-Anlage getrennt sind, und die Anlagen selbst schützen zu können.

Zu § 3:

Das DSG soll auf alle Datenbanken des öffentlichen Bereiches anwendbar sein. Es soll auf alle Datenbanken (und auf die Erhebung personenbezogener Datenbanken) anzuwenden sein, soweit diese von oder im Auftrage eines Rechtsträgers geführt werden, der durch Gesetz eingerichtet ist. Ist die Einrichtung dieser Rechtsträger wenigstens in Vollziehung Landessache, so sind die Bestimmungen des DSG in einer durch § 4 modifizierten Form anzuwenden. Für die Datenverarbeitung aller anderen durch Gesetz einzurichtenden Rechtsträger obliegt seine Vollziehung Bundesbehörden und die Kontrolle seiner Anwendung der Bundes-Datenschutzkommission.

Diese Bezugnahme auf die Einrichtung eines Rechtsträgers durch Gesetz wurde gewählt, um den öffentlichen Bereich abzugrenzen, da dies ein eindeutiges Abgrenzungskriterium darstellt. Es fallen darunter jedenfalls der Bund mit allen seinen Ausgliederungen, Selbstverwaltungskörper (Sozialversicherungsträger, Kammern), der ORF, verschiedene Fonds, die Österreichische Postsparkasse, die Oesterreichische Nationalbank, die ÖIAG, wobei deren Einbeziehung aus dem Wirtschaftspotential, das diesen Rechtsträgern zur Verfügung steht, gerechtfertigt erscheint.

Die gesetzlich anerkannten Kirchen und Religionsgesellschaften fallen nicht unter die Anwendung des DSG gemäß § 3, da sie durch Gesetz zwar anerkannt, aber nicht eingerichtet sind (vgl. Gesetz RGBl. Nr. 68/1874) unter Umständen aber unter §§ 24 bis 26. Die Weitergabe von personenbezogenen Daten ist daher nur unter den Voraussetzungen des § 7 möglich.

Es wurde keine Differenzierung danach vorgenommen, ob die Datenbank zum Zwecke der Privatwirtschafts- oder für Zwecke der Hoheitsverwaltung verwendet wird, da der Schutzzweck des Gesetzes und das Legalitätsprinzip des Art. 18 B-VG es rechtfertigen, auch jene in die Datenbank einzubeziehen. Es ist weiters aus den

Daten bzw. in der Datenbank selbst in der Regel nicht zu trennen, ob sie für hoheitliche oder für privatwirtschaftliche Zwecke verwendet werden.

Die Ausnahme des Abs. 2 der Verarbeitung personenbezogener Daten von oder im Auftrage von Organen des Bundes- oder Landesgesetzgebers (eigene Datenbanken bzw. Datenbanken des Rechnungshofes) ist aus dem Schutzzweck des Gesetzes nicht gerechtfertigt, die Einbeziehung dieser Organe unter das DSG (und damit unter Kontrolle der Verwaltung, vgl. § 9, § 20) bedürfte allerdings einer besonderen verfassungsgesetzlichen Bestimmung.

Die Ausnahme des Abs. 3 für die Österreichische Postsparkasse und die Oesterreichische Nationalbank ist einerseits dadurch gerechtfertigt, daß für diese Kreditunternehmungen gegenüber den diesen Abschnitten des DSG nicht unterliegenden Kreditunternehmungen keine Wettbewerbsverschlechterung eintreten soll, und andererseits, daß etwa das Postsparkassengesetz eine weitreichende Verschwiegenheitspflicht vorsieht (§ 22 Abs. 3 des Postsparkassengesetzes, BGBl. Nr. 458/1969). Wohl aber werden diese Institute den Abschnitten V und VI des DSG unterliegen.

Zu § 4:

Wie bereits im allgemeinen Teil der Erläuterungen ausgeführt wurde, ist es für die Effektivität des Datenschutzes entscheidend, daß gleichartige personenbezogene Daten in allen Datenbanken gleichrangig gesichert sind, daß gegen ihre ungerechtfertigte Verarbeitung, gegen ihre Verfälschung die gleichen Rechtschutzmöglichkeiten zustehen. Daher muß wenigstens ein einheitliches Datenschutzgesetz für den Bereich von Bund, Ländern, Gemeinden oder sonstigen Selbstverwaltungskörpern erlassen werden. Dem Gedanken des Bundesstaates wird aber dadurch Rechnung getragen, daß die Vollziehung des Datenschutzgesetzes den Ländern zusteht, soweit Datenbanken von durch Gesetz eingerichteten Rechtsträgern errichtet oder beauftragt sind, deren Einrichtung in der Vollziehung in die Zuständigkeit der Länder fällt. Dies gilt auch für Datenbanken von Gemeinden und Gemeindeverbänden. Unter § 4 werden daher vor allem Rechtsträger fallen, die kompetenzmäßig Art. 11, 12 und 15 B-VG zugehören. Eine gesonderte Anführung der Gemeindeverbände wurde vorgenommen, da ihre Einrichtung in den einzelnen Gemeindeordnungen unterschiedlich ist, und diese Unterschiede nicht für die Anwendung des DSG von Ausschlag sein sollen.

Die Modifikationen, unter denen das DSG durch Landesbehörden anzuwenden ist, ergeben sich aus § 4 Z. 1 bis 8 und beinhalten vornehmlich Rechte der Landesregierung anstelle von Rechten eines Bundesministers oder der Bundesregierung und die Einrichtung von Landes-Datenschutzkommissionen, die im Geltungsbereich des § 4 die sonst von der Bundes-Datenschutzkommission wahrzunehmenden Zuständigkeiten durchzuführen haben.

Zu § 5:

§ 5 nimmt Datenbanken, auf die die Begriffsbestimmung des § 2 Z. 10 zutrifft, vom Anwendungsbereich dieses Gesetzes aus, die kraft ausdrücklicher bundes- oder landesgesetzlicher Anordnung öffentlich sind. Hier sind als Beispiele das Grundbuch (§ 7 GBG), die Wählerevidenz (§ 3 Abs. 1 Wählerevidenzgesetz 1973), das Handelsregister (§ 9 Abs. 1 HGB) und das Luftfahrzeugregister (§ 16 LuftFG) zu nennen. Diese Bestimmung soll nur zur Anwendung kommen, wenn die ganze Datenbank öffentlich zugänglich ist, die nicht öffentlich zugänglichen Teile der Datenbank würden unter dieses Gesetz fallen (vgl. z. B. § 29 KartG). Ebenfalls unter den Anwendungsbereich dieses Gesetzes fallen jene Datenbanken, in die eingeschränkt durch vom Gesetz normierte Voraussetzungen von Dritten Einsicht genommen werden kann (z. B. § 12 des Meldegesetzes 1972, BGBl. Nr. 30/1973; § 365 der Gewerbeordnung 1973) sowie Datenbanken, die nur auf Grund einer Verordnung öffentlich geführt werden.

Es sei zu dieser Bestimmung noch darauf hingewiesen, daß sehr wohl aus der Umstellung einer konventionell geführten Datenbank, deren Öffentlichkeit zwar vom Gesetz vorgesehen ist, aber durch die faktischen Verhältnisse beschränkt ist, auf EDV Probleme für die Privatsphäre und die Zugänglichkeit personenbezogener Daten auftauchen können, doch werden hier im konkreten Einzelfall gesonderte rechtspolitische Überlegungen anzustellen sein (etwa könnte die Umstellung der österreichischen Grundbücher auf EDV dazu führen, daß die Eigentums- und Belastungsverhältnisse der Grundstücke aller österreichischen Katastralgemeinden zentral abgefragt werden, wozu gegenwärtig die Grundbücher aller Katastralgemeinden aufgesucht werden müßten).

Zu § 6:

Diese Bestimmung erlaubt die Erhebung und Verarbeitung personenbezogener Daten nur unter zwei Voraussetzungen: Der datenverarbeitende Rechtsträger muß hiezu ausdrücklich vom Gesetz ermächtigt sein oder/und die Verarbeitung muß wesentliche Voraussetzung der Durchführung der diesem Rechtsträger gesetzlich übertragenen Aufgaben der Hoheits- oder Privatwirtschaftsverwaltung im eigenen oder übertragenen Wirkungsbereich bilden. Die Datenerhebung und die unter § 2 Z. 3 genannten Komponenten der Datenverarbeitung werden

damit, soweit sie personenbezogene Daten betreffen, nicht mehr in die freie Entscheidung der Behörde gestellt, sondern explizit den Bedingungen des Gesetzmäßigkeitsprinzipes unterworfen. Die ausdrückliche gesetzliche Ermächtigung muß jede der Komponenten der Datenverarbeitung umfassen und auch die zugelassenen Daten ausdrücklich bezeichnen.

Die zweite mögliche Voraussetzung enthält die Zulässigkeit der Verarbeitung personenbezogener Daten insoweit, als ohne eine solche Verarbeitung die Wahrnehmung der diesem Rechtsträger obliegenden Aufgaben nicht möglich wäre. Sie wird sich also auf jene personenbezogenen Daten und auf jene Komponenten der Datenverarbeitung zu beschränken haben, die unmittelbar in die Tätigkeit dieser Behörde, Dienststelle u. ä. einfließen. Nach § 6 sollen etwa zulässig sein die Datenbanken, die von Polizeibehörden zur Wahrung der öffentlichen Sicherheit eingerichtet sind, die der Militärkommandos für die Personaldaten der Wehrpflichtigen, die Datenbanken der Interessenvertretungen für die Evidenthaltung der Mitglieder und deren gesetzlicher Verpflichtungen und ähnliches.

§ 6 selbst gibt nur die grundsätzliche Berechtigung für die Datenverarbeitung; ihre Beschränkung besonders hinsichtlich der Geheimhaltungspflicht und des Weitergabeverbotes enthalten einerseits die folgenden Bestimmungen dieser Vorlage und andererseits die materiellen Bestimmungen, die die Datenverarbeitung zulassen; welche Behörde innerhalb des Rechtsträgers für die Verarbeitung solcher Daten zuständig ist, ergibt sich aus den entsprechenden Zuständigkeitsbestimmungen.

Zu § 7:

Der Entwurf muß darauf Rücksicht nehmen, daß mit Inkrafttreten des Bundesministeriengesetzes 1973 durch die im Zuge der parlamentarischen Beratungen eingefügten Bestimmungen des § 3 Z. 5 und des § 4 Abs. 3 zumindest für den Bereich der unmittelbaren Bundesverwaltung der Grundsatz der allgemeinen Auskunftspflicht der Behörden eingeführt wurde. Der vorliegende Entwurf beschränkt sich daher in Übereinstimmung mit den zitierten Bestimmungen des Bundesministeriengesetzes auf einen Schutz aller unter das Amtsgeheimnis fallenden Daten. Ein Verbot der Weitergabe auch von nicht unter das Amtsgeheimnis fallenden Daten wäre übrigens nach Art. 20 Abs. 3 B-VG problematisch, weil eine derartige Regelung einer verfassungswidrigen Erweiterung der Amtsverschwiegenheit gleichkäme (vgl. das Erkenntnis des Verfassungsgerichtshofes Slg. 6288/1970).

Daten, die der Amtsverschwiegenheit oder einer gesetzlich normierten Verschwiegenheitspflicht unterliegen, dürfen grundsätzlich nicht weitergegeben werden. Von diesem Grundsatz, der auch gegenüber anderen Behörden und Rechtsträgern gilt, sind nur drei Ausnahmen vorgesehen (Ausnahmen von der Amtsverschwiegenheit sind durch einfache Gesetze möglich, vgl. das letztzitierte Erkenntnis des Verfassungsgerichtshofes):

a) soweit gesetzlich etwas anderes bestimmt ist; etwa für den Bereich der Amts- und Rechtshilfe (z. B. Art. 22 B-VG; § 9 des Strafregistergesetzes 1968, § 6 des Tilgungsgesetzes 1972; § 41 des Wiener Sozialhilfegesetzes, LGBl. Nr. 11/1973; § 360 ASVG); oder für Auskünfte Dritten gegenüber (z. B. § 12 Meldegesetz; § 118 Abs. 2, letzter Satz BAO; § 13 des Bundesgesetzes über äußere Rechtsverhältnisse der Evangelischen Kirche, BGBl. Nr. 182/1961; § 458 ASVG);
b) bei personenbezogenen Daten, deren Geheimhaltung ausschließlich im Interesse des Betroffenen geboten ist,
   aa) wenn der Betroffene der Weitergabe schriftlich zugestimmt hat oder
   bb) wenn durch geeignete Maßnahmen bei der Weitergabe sichergestellt wird, daß der Betroffene nicht mehr bestimmbar ist. Durch diese Bestimmung des Abs. 2 Z. 2 soll insbesondere die Auswertung von Datenbanken mit Individualdaten für Zwecke der Statistik ermöglicht werden. Allerdings wird eine bloße Aggregierung von Einzeldaten nicht den Anforderungen dieser Bestimmung genügen, sondern nur eine Anonymisierung, der Ausschluß der Rückführbarkeit des Einzeldatums auf den Betroffenen (vgl. § 9 Abs. 3).

Eine Weitergabe von der Amtsverschwiegenheit unterliegenden personenbezogenen Daten, deren Geheimhaltungsinteresse nicht ausschließlich beim Betroffenen, sondern bei Dritten liegt, ist daher nur auf Grund ausdrücklicher gesetzlicher Ermächtigung zulässig.

Im Zuge der Ausarbeitung dieser Regierungsvorlage wurde auch eine Erhebung über die in den geltenden Bundes- und Landesgesetzen enthaltenen Verschwiegenheitspflichten und die Durchführungsbestimmungen zu Art. 22 B-VG vorgenommen, doch waren im Zeitpunkt der Einbringung dieser Regierungsvorlage noch nicht die Stellungnahmen aller ersuchten Stellen eingelangt, sodaß Listen der Bestimmung, auf die § 7 DSG im Sinne einer Ausnahme verweist, bzw. der Bestimmungen, die Daten den Verschwiegenheitspflichten nach § 7 DSG unterwerfen, noch nicht erstellt werden konnten.

In Entsprechung zu den Voraussetzungen für die Datenerhebung und -verarbeitung enthält Abs. 3 als Durchführung zu Art. 22 B-VG die

Möglichkeit der Datenweitergabe, wenn diese für das empfangende Organ eine wesentliche, notwendige Voraussetzung zur Durchführung ihm gesetzlich übertragener Aufgaben der Hoheits- und Privatwirtschaftsverwaltung ist; es soll etwa der Datenverkehr zwischen einer Kammer und einem Bundesministerium für Zwecke der Förderungsverwaltung nicht behindert werden.

Den Abgeordneten des Nationalrates und den Mitgliedern des Bundesrates dürfen personenbezogene Daten im Rahmen der Bestimmungen des Art. 52 und des Art. 53 B-VG weitergegeben werden.

Zu § 8:

Das Verbot der Verknüpfung personenbezogener Daten ist eines der zentralen Anliegen aller Datenschutzgesetzgeber, da aus der Verbindung von für verschiedene Zwecke und/oder an verschiedenen Stellen ermittelte oder gespeicherte Daten sich gerade die Möglichkeit der Erstellung von Persönlichkeitsbildern ergibt, die sich aus einer Mehrzahl ursprünglich unzusammenhängender Individualdaten zusammenstellen lassen und eine Verwaltungsentscheidung unbewußt in einer Richtung beeinflussen können, die mit den Zielen dieses Verwaltungszweiges keinen Konnex hat.

Da sich aus der Definition des § 2 Z. 7 ergibt, daß unter Verknüpfung sowohl das einmalige als auch das dauernde Zusammenfassen zu verstehen ist, müssen die Voraussetzungen des § 8 vorliegen, wenn im Einzelfall, etwa bei Klärung einer Vorfrage von einem amtshandelnden Organ auf Daten aus einer anderen Datenbank (d. h. einer Datenbank, die von einer anderen Behörde geführt oder beauftragt ist; es ist durchaus denkbar, daß in einem Computer mehrere Datenbanken im Sinne dieser Regierungsvorlage verarbeitet werden, entscheidend ist die programmtechnische Einrichtung einer Sammlung personenbezogener Daten und deren Führung durch die gesetzmäßig zuständige Stelle) zurückgegriffen werden soll. Es muß sowohl dafür als auch für das dauernde Zusammenfassen der Daten eine ausdrückliche gesetzliche Ermächtigung vorliegen, bzw. die Verknüpfung muß mit dem Zweck, für den die Daten ermittelt wurden, vereinbar sein. Der Zweck der Datenermittlung (der Begriff ist weiter als der des § 2 Z. 4, er erfaßt auch das Sammeln von Daten ohne Mitwirkung des Betroffenen) und der Datenverarbeitung wird sich anbetracht des Grundsatzes der Gesetzmäßigkeit der Verwaltung aus dem gesetzlichen Zuständigkeitsbereich der die Datenbank führenden Stellen ermitteln lassen; es wird grundsätzlich davon auszugehen sein, daß eine Behörde Daten nur im Rahmen ihres gesetzlichen Zuständigkeitsbereiches ermitteln und verarbeiten darf, worunter auch der Fall fällt, in dem eine Behörde durch Gesetz verpflichtet wird, für eine andere Behörde Daten zu erheben bzw. zu verarbeiten.

Das Verbot der Verknüpfung personenbezogener Daten ist unabhängig von der Interessenlage des konkreten Falles und gilt daher für alle Daten ohne Rücksicht darauf, ob sie einem Amtsgeheimnis unterliegen oder nicht.

Zu § 9:

Dem § 9 vergleichbare Bestimmungen finden sich in allen Entwürfen zum Datenschutz, da ein allgemeines Datenschutzgesetz wohl generelle Regelungen und die Rechtsgrundlage für den Datenschutz geben kann, aber die konkreten Schutzbestimmungen, insbesondere der technischen Seite des Datenschutzes (Datensicherung) nur für jede einzelne Datenbank vorgenommen werden können. Teils werden in diesen Dokumenten nur die Verpflichtungen zur Erlassung von Betriebsordnungen statuiert (Art. 6 des schwedischen Datenschutzgesetzes; Art. 10 des luxemburgischen Gesetzentwurfes für ein Regierungsinformationszentrum, Chambre de Députés n° 1684 vom 10. April 1973), teils ist im Gesetz bereits der notwendige Inhalt derartiger Betriebsordnungen vorgegeben (z. B. § 4 der Regierungsvorlage der deutschen Bundesregierung). Im Hinblick auf Art. 18 Abs. 2 B-VG war für Österreich nur der zweite Weg gangbar, sodaß § 9 den Inhalt der Datenbank-Verordnungen detailiert umschreibt. Schutzobjekt einer derartigen Verordnung ist das ganze Datenbanksystem (vgl. die Definition von Datenbank im § 2 Z. 10), also die technischen Einrichtungen einschließlich der Gebäude, das Personal, sowie die Datenträger, auch wenn sie gegenwärtig nicht mit der EDV-Anlage verbunden sind, neben den Schutz der Daten tritt der der Datenträger und des Computers. Die Datenbank-Verordnungen können als ein Mindest-Standard der Datensicherung angesehen werden, an dessen Verletzung sich rechtliche Sanktionen knüpfen. Inwieweit aus betrieblichen Gründen darüber hinaus weitere Sicherheitsrichtlinien zu erlassen sind, obliegt der die Datenbank bzw. die EDV-Anlage führenden Stelle.

§ 9 sieht für jede Datenbank eine in Form einer Verordnung zu erlassende Betriebsordnung vor. Zuständig zur Erlassung ist nach Anhörung des Bundeskanzlers (§ 5 Abs. 1 Z. 2 des Bundesministeriengesetzes 1973), die in der Berührung der Grundrechtssphäre begründet ist, der Bundesminister (bzw. die Landesregierung, § 4 Z. 1), der der die Datenbank führenden Dienststelle übergeordnet ist, bzw. der gegenüber dem die Datenbank führenden Selbstverwaltungskörper das Aufsichtsrecht hat. Wegen der Bedeutung des Datenschutzes in Zusammenhang mit den Grundrechten wird ein Verordnungsrecht des Bundesministers auch für die Datenbanken der Selbstverwaltungskörper vorgesehen.

Bei Zweifeln über die Zuständigkeit eines Bundesministers wird diese primär nach der die

EDV-Anlage organisatorisch bzw. personell betreuenden Stelle zu beurteilen sein. Im Falle der Zusammenarbeit mehrerer Bundesministerien in einer EDV-Anlage wird die Datenbank-Verordnung im Zusammenwirken der betreffenden Bundesminister (§ 5 des Bundesministeriengesetzes) zu erlassen sein.

In diesen Verordnungen werden vor allem möglichst konkrete Bestimmungen über die Pflichten enthalten sein müssen, die von den die Datenbank führenden Stellen und von dem mit der Datenbank und den Daten beschäftigten Personen zu beachten sind sowie über personelle, technische, bauliche und organisatorische Sicherungen („Orgware", vgl. P. Lindemann — K. Nagel — C. Hermann, Organisation des Datenschutzes, 1973, S. 30 ff.), die eine beabsichtigte, aber gesetzwidrige oder eine unbeabsichtigte (zufällige) Weitergabe, Veränderung (Verfälschung), Verbindung oder Löschung von Daten ausschließen sollen. Der Inhalt der Sicherungsvorschriften wird einerseits abhängen von den technischen Möglichkeiten und der wirtschaftlichen Vertretbarkeit, der Sicherung — was letztlich eine Kostenabwägung ist — andererseits von der Art der in der Datenbank gespeicherten Daten. Je sensibler die verarbeitenden personenbezogenen Daten sind, d. h. je eher sie der Privat- oder Intimsphäre zuzurechnen ist, oder je eher ihre Weitergabe bzw. Löschung berechtigte Interessen des Betroffenen oder der speichernden Stelle verletzen kann, desto strenger werden die Sicherungsvorschriften sein müssen. In einer EDV-unterstützten Datenbank werden in den Betriebsordnungen insbesondere Schutzbestimmungen für den Zugang zur Hardware (z. B. Absperrung des Raumes) einschließlich der Benützung der Terminals (z. B. Vorschrift von Benützercodes oder physischen Charakterisierungen wie Fingerabdrücken, Stimmvergleichen oder Unterschriften, magnetische Identifikationskartensysteme u. ä.) sowie gegen die Veränderung der Software (Programme) durch das Bedienungspersonal enthalten sein müssen. Die Datenbank-Verordnungen werden auch auf das Speichern Bezug zu nehmen haben, soweit damit eine Datenweitergabe oder Datenveränderung ermöglicht würde.

In Abs. 2 werden demonstrativ die in einer Datenbank-Verordnung notwendigen Bestimmungen angeführt, wobei die Einhaltung dieser Bestimmungen von der Bundes-Datenschutzkommission zu überwachen sein wird (§ 20, § 21). Hiezu ist vor allem eine Protokollierungspflicht aller Datenweitergaben (worunter auch die Datenverknüpfung fallen wird, da diese in der Mehrheit der Fälle auch eine Datenweitergabe beinhaltet) vorgesehen, da nur über sie der Berichtigungsanspruch des § 11 Abs. 2 verfolgbar ist. Unter „Protokoll" ist nicht allein ein Papierausdruck zu verstehen, sondern es reicht eine interne Protokollierung aus, die im Bedarfsfall abgerufen werden kann. Je nach Bedeutung der Daten wird eine Aufbewahrung für diese Protokolle vorzusehen sein, wobei dieser Zeitraum je länger sein soll, je eher durch die Weitergabe unrichtiger Daten berechtigte Interessen verletzt werden könnten.

Die Datenbank-Verordnung sollte auch Bestimmungen enthalten über die Berechtigung zum Zugriff zur Datenbank und über die einzelnen Berechtigungen der bei ihr tätigen Personen, die je nach Tätigkeitsbereichen unterschiedlich sein werden. Es sollen auch die Personen zur Geheimhaltungspflicht verhalten werden, die nicht der Amtsverschwiegenheit unterliegen.

Bei Weitergabe zu statistischen oder wissenschaftlichen Zwecken (§ 7 Abs. 2 Z. 3) ist sicherzustellen, daß die Daten nur in einer solchen Form weitergegeben werden, daß ihre Rückführbarkeit auf den Betroffenen nicht mehr möglich ist (Abs. 3). Diese Anonymisierung wird zu erfolgen haben durch Löschen z. B. des Namens und des Geburtsdatums im Datensatz, des Personenkennzeichens, der Sozialversicherungsnummer u. ä., sie wird auch dann vorliegen, wenn zwar mit individuellen Merkmalen ermittelte Daten nur ohne diese gespeichert und weitergegeben werden.

In der Datenbank-Betriebsordnung wird auch zu regeln sein, daß die gesetzmäßige Weitergabe von Daten unter möglichstem Ausschluß der Gefährdung berechtigter Interessen der Betroffenen erfolgt (Abs. 3). Was „berechtigte Interessen" sind, wird je nach weitergegebenen Daten und nach dem Kreis der empfangsberechtigten Personen unterschiedlich sein. Die Vorkehrungen werden jedenfalls umso strikter sein müssen, je eher die weitergegebenen Daten der Intimsphäre des Menschen zuzurechnen sind.

In Abs. 4 wird der die Datenbank-Verordnung erlassenden Stelle die Pflicht auferlegt, diese der technischen Entwicklung anzupassen. Diese Bestimmung scheint notwendig, da sich die Datenverarbeitungstechnik sehr rasch entwickelt und immer neue Methoden der Datensicherung eingeführt werden, von denen im Interesse der Privatsphäre unter den Voraussetzungen der technischen und kostenmäßigen Praktikabilität Gebrauch gemacht werden sollte.

Zu § 10:

Der Betroffene, d. h. die Person, auf die sich die verarbeiteten personenbezogenen Daten beziehen, hat einen Rechtsanspruch auf Bekanntgabe der ihn betreffenden gespeicherten Daten selbst dann, wenn sie an sich der Amtsverschwiegenheit unterliegen. Dieser Rechtsanspruch ist nur in jenen Fällen ausgeschlossen, in denen dies durch eine besondere gesetzliche Vorschrift aus-

drücklich angeordnet ist oder im Interesse einer Gebietskörperschaft liegt. Solche gesetzliche Vorschriften sind z. B. § 17 Abs. 2 AVG und § 90 Abs. 2 BAO.

Das Interesse einer Gebietskörperschaft wird insbesondere dann gegeben sein, wenn durch die Bekanntgabe der Daten der Zweck eines staatlichen Aktes vereitelt würde (z. B. Entziehung der Strafverfolgung). Die Entsprechung eines Antrages auf Auskunftserteilung hat in Form eines unverschlüsselten Textes und schriftlich zu erfolgen.

Die Verpflichtung zur Mitteilung der Rechtsgrundlage der Erhebung und Verarbeitung wurde statuiert, um den Betroffenen die Möglichkeit der Information über die Rechtmäßigkeit der Handlungen in der Datenbank zu geben, und um ihm bei der Prüfung, ob ein Berichtigungsantrag bzw. eine Beschwerde bei der Bundes-Datenschutzkommission erhoben werden soll, zu helfen.

Es ist die Absicht des Entwurfes, daß über einen Antrag auf Auskunft nach § 10 nicht ein mit Bescheid abzuschließendes Verwaltungsverfahren nach dem AVG oder ähnlichen Bestimmungen durchzuführen, sondern dem Betroffenen eine formlose Mitteilung zuzustellen ist, in der ihm entweder die gewünschte Auskunft erteilt wird oder die Verweigerung der Auskunft schriftlich zu begründen ist. Dieser Weg wurde nicht nur aus verwaltungsökonomischen Erwägungen gewählt (häufig werden solche Auskünfte unmittelbar im Wege eines Computer-Ausdruckes geschehen können), sondern auch deswegen, weil einer Reihe datenverarbeitender Einrichtungen keine Behördenqualität zukommt. Der Rechtsanspruch auf Erteilung einer Auskunft ist somit auch nicht bei der der datenverarbeitenden Einrichtung übergeordneten Instanz, sondern im Wege einer Beschwerde bei der Bundes-Datenschutzkommission (§ 20) geltend zu machen.

Die Datenschutzgesetze bzw. -entwürfe des Auslandes sehen eine Beschränkung der Auskunftspflicht auf einmalige Auskunft innerhalb eines bestimmten Zeitraumes (§ 10 des schwedischen Datenschutzgesetzes: zwölf Monate) oder eine Gebührenpflicht für eine Auskunftserteilung vor (§ 11 Abs. 4 des Entwurfes der deutschen Bundesregierung; Art. 7 Abs. 4 des Initiativantrages der SPD im bayrischen Landtag), um die grundlose und allzuhäufige Geltendmachung des Auskunftsrechtes faktisch zu beschränken. Die Verpflichtung zur Auskunftserteilung kann nämlich bei häufiger Inanspruchnahme des Auskunftsrechtes zu einem wesentlichen Kostenelement der Datenverarbeitung werden, sodaß hier die Möglichkeit geschaffen werden muß, den Kosten einer Auskunftserteilung entsprechende Verwaltungsabgaben — die die tatsächlichen Kosten der Auskunft aber nicht überschreiten wird — einzuheben. Von dieser Möglichkeit sollte aber nur Gebrauch gemacht werden, wenn die Einräumung des Auskunftsrechtes die Aufwendungen für die Datenbank wesentlich erhöht was sich primär aus der Zahl der Auskunftsansuchen ergeben wird, die gegenwärtig nicht abschätzbar ist.

Eine weitere Ausnahme von der Auskunftspflicht der Datenbank ist dann gegeben, wenn die Daten dem Betroffenen bereits mitgeteilt wurden (etwa: regelmäßige Zusendung von Lastschriftanzeigen), da verwaltungsökonomischer Grundgedanke sein muß, nur zu einer einmaligen Auskunft über dasselbe Datum zu verpflichten; ändert sich das Datum in der Datenbank, so besteht die Auskunftspflicht wieder.

Zu § 11:

Dem Auskunftsrecht des Betroffenen hat eine ebenso im Rechtsweg (§ 20) durchsetzbare Berichtigungspflicht der datenverarbeitenden Stelle zu entsprechen. Die die Datenbank beauftragende Stelle (es wird dies die Stelle sein, die für die Dateneingabe verantwortlich ist) hat auf Antrag des Betroffenen, von Amts wegen (wenn Zweifel an der Richtigkeit eines Datums auftreten) sowie auf Grund einer Entscheidung der für die Feststellung der Daten sachlich zuständigen Behörde oder auf Auftrag einer Datenschutzkommission (§ 19 Abs. 5) unrichtige Daten zu berichtigen, unvollständige Daten (z. B. daß gegen eine Entscheidung einer Disziplinarbehörde ein Rechtsmittel eingelegt wurde) zu ergänzen und überholte Daten (z. B. daß eine Lohnpfändung bereits beendet ist) zu löschen. Der Begriff der Unrichtigkeit umfaßt auch überholte Daten. Von der Berichtigungspflicht sind auch jene Daten betroffen, die ohne gesetzliche Grundlage oder ohne daß sie eine wesentliche Voraussetzung für die diesem Rechtsträger obliegende Vollziehung (§ 6) bilden, verarbeitet wurden. Die Beweislast für die Richtigkeit bzw. Vollständigkeit der Daten sowie für die Berechtigung ihrer Verarbeitung obliegt der datenverarbeitenden Einrichtung, es sei denn, daß die Daten unter Mitwirkung des Betroffenen ermittelt wurden (Erhebung im Sinne des § 2 Z. 4); die datenverarbeitenden Stellen sollen sich um die Richtigkeit selbständig ermittelter Daten bemühen.

Über Anträge nach § 11 soll die die Datenbank beauftragende Einrichtung nicht bescheidmäßig absprechen, auch nicht im Falle einer Verweigerung einer Berichtigung. Es soll aus verwaltungsökonomischen Gründen in der Regel kein Verwaltungsverfahren durchgeführt werden, sondern die Einrichtung kann die beantragte Handlung innerhalb der vorgesehenen Frist durchführen und wird dies dem Antragsteller mitzuteilen haben; geschieht dies innerhalb der Frist nicht, so steht dem Antragsteller gegen

die Verweigerung oder gegen die Säumigkeit kein Rechtsmittel zu (vgl. die Konstruktion des § 17 AVG und VwGH Slg. 1623 A/1950), sondern nur die Möglichkeit einer Beschwerde an die zuständige Datenschutzkommission nach § 20 (vgl. auch die Erläuterungen zu § 20). Die Klärung der der Datenverarbeitung zugrundezulegenden Angaben hat unverzüglich zu erfolgen (Abs. 1, letzter Satz), was ebenfalls von der Datenschutzkommission überprüft werden kann.

Die Bestimmungen des Abs. 4 ergeben sich aus der Notwendigkeit, daß der Betroffene Kenntnis von der vorgenommenen Berichtigung bzw. daß die Datenschutzkommission Kenntnis von der Durchführung ihrer Entscheidung erhält, die des Abs. 5 aus einer Interessenabwägung zwischen den Einzelinteressen des Betroffenen und den Grundsätzen der Sparsamkeit und Zweckmäßigkeit der Verwaltung, da eine unbegrenzte Rückwärtsdokumentation und -berichtigung kostenmäßig nicht vertretbar ist. Die Feststellbarkeit des Empfängers wird sich meist in Relation aus der Aufbewahrungspflicht der Protokolle der Weitergaben (§ 9 Abs. 2) ergeben.

Eine Benachrichtigung des Betroffenen nach Abs. 4 ist nicht vorgesehen, wenn ihm die vorgenommene Berichtigung bzw. Löschung bereits von der Behörde, die für die Feststellung der Daten sachlich zuständig ist, mitgeteilt wurde (etwa anläßlich der Entscheidung über ein vom Betroffenen in der Sache erhobenes Rechtsmittel).

Abs. 6 soll klarstellen, daß Daten, bei deren Ermittlung auf ihre Richtigkeit zu einem bestimmten Zeitpunkt abgestellt wurde (z. B. Volkszählung, statistische Erhebungen) später nicht gemäß § 11 zu korrigieren sind, auch wenn sich der zugrunde gelegte Sachverhalt geändert hat. Dieser Zweck wird sich in der Regel aus dem die Ermittlung oder Verarbeitung zulassenden Rechtsvorschriften ergeben.

Abs. 7 verpflichtet die die Datenbank führende Behörde einerseits explizit zur Durchführung von Entscheidungen über in der Datenbank gespeicherte Daten im Sinne einer Löschung oder Berichtigung, wenn sich dies aus der Entscheidung ergibt, und andererseits ist diese Einrichtung auch bei einem Berichtigungsantrag des Betroffenen an diese Entscheidung gebunden.

Zu § 12:

Diese Bestimmung sieht eine Ausnahme für das von der Bundespolizeidirektion Wien geführte Strafregister vor, auf das in seiner gegenwärtigen Durchführung zwar die Begriffsumschreibung des § 2 Z. 10 zutrifft, und auf das daher die Bestimmungen des Datenschutzgesetzes grundsätzlich anzuwenden sind, bei dem aber § 3 und § 10 des Strafregistergesetzes einen dem Auskunfts- und Berichtigungsrecht des Datenschutzgesetzes entsprechenden Rechtsanspruch gewähren. Um hier ein zu Rechtsunklarheiten führendes Nebeneinander der entsprechenden Bestimmungen des Strafregistergesetzes und des Datenschutzgesetzes zu verhindern, wird das Strafregister hinsichtlich des Auskunfts- und des Berichtigungsrechtes von der Anwendung des Datenschutzgesetzes ausgenommen. Gegen eine unmittelbare Auskunftserteilung aus dem Strafregister an den Betroffenen (und nicht nur, wie in § 10 des Strafregistergesetzes, im Wege der Gemeinde) spricht auch, daß ein zu leichtes Erlangen von Strafregisterbescheinigungen den Wunsch zur Beibringung derartiger Auskünfte in verstärktem und ungerechtfertigtem Maße hervorrufen würde, wie die Überlegungen zum deutschen Bundes-Zentralregistergesetz (dBGBl. 1971 I S. 243) zeigen.

Beruft sich aber ein Betroffener auf eine Verletzung des Datenschutzgesetzes, so ist, abgesehen von den Fällen des § 10 und § 11, die Bundes-Datenschutzkommission zur Entscheidung berufen.

Zu § 13:

Ein Recht auf Auskunft über Daten kann nur dann für den Betroffenen seinen Zweck erfüllen, wenn für ihn die Möglichkeit der Kenntnis der datenverarbeitenden Stellen besteht. Daher müssen die Datenbanken der öffentlichen Hand periodisch der Öffentlichkeit bekanntgegeben werden. Für die Abschätzung der sich für Betroffene aus der Datenverarbeitung ergebenden möglichen Gefahren reicht aber nicht die bloße Kenntnis aus, daß und wo Datenbanken errichtet sind, sondern es muß auch der Kreis der Betroffenen (etwa alle Bewohner der Gemeinde M; alle männlichen Staatsbürger über 18 Jahre; alle Führerscheinbesitzer u. ä.) und die Art der verarbeiteten personenbezogenen Daten (Personaldaten, Adressen, Sozialversicherungsnummer, monatliches Einkommen usw.) und der Zweck der Datenbank (z. B. Hörerevidenz und Hochschulstatistik) veröffentlicht werden. Diese Publizierung muß übersichtlich erfolgen, d. h. in einem Kundmachungsorgan und möglichst für alle Datenbanken gleichzeitig und unabhängig davon, ob die Datenverarbeitung unmittelbar bei öffentlichen Stellen oder nur in deren Auftrag durchgeführt wird. Daher wird, auch in Entsprechung des Verlautbarungsgesetzes 1945, eine Verlautbarung der Datenbanken, die von öffentlichen Stellen oder in deren Auftrag (§ 14 Abs. 3) geführt werden, im Amtsblatt zur Wiener Zeitung vorgesehen (für die Landes-Datenschutzkommissionen vgl. § 4 Z. 2, 3). Die Unterlassung, Unrichtigkeit oder Unvollständigkeit dieser Verlautbarung könnte zum Gegenstand einer Beschwerde nach § 20 werden.

Die Verlautbarung der Datenbanken obliegt dem Bundeskanzleramt; von einer Verlautbarung durch die Datenschutzkommission wurde abgesehen, da es zweifelhaft sein mag, ob einer Behörde nach Art. 133 Z. 4 B-VG andere Aufgaben als Entscheidungen in Verwaltungssachen übertragen werden können. Dem Bundeskanzleramt müssen die Datenbanken, der Kreis der Betroffenen, die Art der verarbeiteten Daten zeitgerecht vor der Veröffentlichung mitgeteilt werden; diese Mitteilung soll auch nicht für die Veröffentlichung bestimmte Hinweise über die Rechtsgrundlage (vgl. aber deren Mitteilung an den Auskunftsberechtigten gemäß § 10 Abs. 1) und die Verwendung der Datenbank enthalten, um die Praxis der Datenbanken auch außerhalb von individuellen Anlaßfällen zusammenzufassen und für die Zukunft, dem Gedanken der Koordinierung Rechnung tragend, legistische und verwaltungstechnische Hilfen zu erhalten.

Zu § 14:

Der Schutz gegenüber der Verarbeitung personenbezogener Daten unmittelbar durch die öffentlichen Stellen muß ergänzt werden durch möglichst entsprechende Vorkehrungen gegenüber der Verarbeitung personenbezogener Daten durch Stellen, deren sich die Vollziehung für den Aufbau und den Betrieb von Datenbanken bedienen kann, und gegen die nicht die gegen die Verwaltung zustehenden Rechtsbehelfe gegeben sind, da sonst ein Ausweichen öffentlicher Stellen besonders hinsichtlich sensibler Daten zu nicht unmittelbar dem Datenschutzgesetz unterliegenden Rechtsträgern und Personen zu befürchten wäre. Auf eine Einbeziehung auch der Erhebung personenbezogener Daten (§ 2 Z. 4) wurde hier verzichtet, da den Auftragnehmern in der Regel keine Sanktionsmöglichkeiten gegen die Verweigerung der Mitwirkung an der Datenermittlung gegeben sind. § 14 enthält den Grundsatz, daß eine Behörde, die personenbezogene Daten durch andere Stellen (z. B. Behörden eines anderen Rechtsträgers mit freier Datenverarbeitungskapazität oder gemeinsame Rechenzentren, Vergabe an private Unternehmen) zur Verarbeitung weitergibt, für den Schutz der Daten verantwortlich bleibt. Diese Verantwortung ist dadurch sicherzustellen, daß in dem Vertrag, mit dem die Verarbeitung personenbezogener Daten in Auftrag gegeben wird (an andere öffentliche Stellen oder an Private) Bestimmungen aufzunehmen sind, die denen der §§ 7 bis 13 entsprechen. Die in § 3 und in § 4 bezogenen Stellen dürfen derartige Verträge überhaupt nur abschließen, wenn sie zur Verarbeitung dieser Daten auf Grund der Bestimmungen des § 6 und der materiellen Zuständigkeitsvorschriften berechtigt sind. Dem Betroffenen soll wohl auch gegenüber derartigen Datenbanken ein Auskunftsrecht und ein Berichtigungsanspruch zukommen, doch wird dies nicht im Verwaltungswege durchsetzbar sein, sodaß ein Rechtsanspruch nur über den Vertrag zwischen Datenverarbeiter und Auftraggeber bestehen könnte. Gegen die auftraggebende Stelle kann, etwa wenn sich diese nicht der ihr zur Verfügung stehenden zivilrechtlichen Möglichkeiten gegen den Auftraggeber bedient, eine Beschwerde gemäß § 20 erhoben werden. Hinsichtlich der Berichtigungspflicht ist die die Datenverarbeitung in Auftrag gebende Einrichtung verpflichtet, die dem Gesetz entsprechende Berichtigung zu veranlassen (§ 11 Abs. 1).

Die Verarbeitung personenbezogener Daten für eine Behörde durch eine andere Behörde oder sonstige organisatorische Einrichtung desselben Rechtsträgers (z. B. EDV-Anlage eines Bundesministeriums für die Datenverarbeitung für ein anderes Bundesministerium) unterliegt nicht den Bestimmungen des § 14, sondern ist allein nach den Bestimmungen der §§ 6 ff. zu beurteilen.

Eine derartige Auftragsvergabe ist denkbar für einzelne Tätigkeiten innerhalb der Verarbeitung in einer Datenbank (zeitlich und/oder sachlich beschränkt, z. B. Vergabe der Speicherungsarbeiten nach einer Volkszählung) oder für den vollen Betrieb einer Datenbank, sie ist denkbar gegenüber privaten oder gegenüber anderen öffentlichen Stellen.

Abs. 3 bestimmt, daß auch derartige Datenverarbeitung in Auftragsform grundsätzlich der Verlautbarungspflicht unterliegt. Davon ausgenommen soll nur die kurzzeitige Vergabe einzelner Tätigkeiten sein (z. B. bei Kapazitätsenge einmaliges Ausweichen auf eine fremde Anlage), wobei als Richtlinie herangezogen werden könnte, daß die Tätigkeit im Berichtszeitpunkt des § 13 nicht mehr andauert und weniger als ein Monat während eines Jahres währte.

Zu § 15:

Für den organisatorischen Schutz der Verarbeitung personenbezogener Daten wird in den ausländischen Dokumenten die Einrichtung einer von der Verwaltung und den die Datenbanken führenden Stellen möglichst unabhängigen Instanz vorgesehen. Als erstes Beispiel ist hier der Datenschutzbeauftragte des Datenschutzgesetzes des deutschen Bundeslandes Hessen (GVBl. 1970 I, S. 625) zu nennen, der als dem Gesetzgeber zugeordnetes und von der Verwaltung getrenntes Organ ein Aufsichts- und Einschaurecht in den Landesdatenbanken hat, er erstattet jährlichen Bericht über seine Erfahrungen an den Landtag (vgl. zuletzt Drucksache 7/5146 des Hessischen Landtages vom 1. April 1974) und kann auch von einzelnen Betroffenen wegen beobachteter Mißstände in Landes-Datenbanken angerufen werden, eine rechtliche Entscheidung und Befehlszuständigkeit hat er aber ebensowenig wie die Datenaufsichtsbehörde des schwedischen Datenschutzgesetzes (Datalag, SFS 1973/289).

Die Regierungsvorlage der österreichischen Bundesregierung ist der erste Entwurf eines Datenschutzgesetzes, mit dem eine Behörde über der staatlichen Verwaltung eingerichtet wird, bei der alle Zuständigkeiten zur Prüfung von Verletzungen dieses Gesetzes und der auf Grund des Gesetzes durchgeführten Verarbeitung personenbezogener Daten konzentriert sind (für den Bund und für den Bereich der einzelnen Bundesländer), und bei der der einzelne Betroffene einen Rechtsanspruch auf Entscheidung über eine von ihm behauptete Rechtsverletzung hat. Den sich aus dem Datenschutz ergebenden spezifischen Rechtsschutzbedürfnissen entsprechend wird hier erstmals in der internationalen Datenschutzdiskussion ein gerichtliches Organ zur Entscheidung über Individualbeschwerden vorgeschlagen.

Für die österreichische Rechtsordnung bietet sich für eine derartige Lösung eine Behörde nach Art. 133 Z. 4 B-VG an, da diese Behörde von den die Datenbank führenden Stellen der Vollziehung oder der Gesetzgebung unabhängig gestellt werden kann, ihr Richter angehören und gegen ihre Entscheidungen die Gerichtshöfe des öffentlichen Rechtes angerufen werden können. Eine derartige Behörde hat auch den Anforderungen an ein Tribunal im Sinne des Art. 6 Abs. 1 der Europäischen Menschenrechtskonvention (vgl. zuletzt VfGH G 30/73 vom 19. März 1974) zu entsprechen, da es nicht auszuschließen ist, daß derartige Behörden über zivilrechtliche Ansprüche zu entscheiden haben. Aus der Entscheidung für die Einrichtung einer Behörde nach Art. 133 Z. 4 B-VG ergeben sich die Bestimmungen des § 15, wobei vor allem auch auf die Möglichkeit Bedacht genommen wurde, Sachverständige der Datenverarbeitung zu Mitgliedern dieser Behörde zu bestellen.

Von der Möglichkeit, für jede Datenbank einen „Datenschutzbeauftragten" vorzusehen, wird abgesehen, da die Tätigkeit eines derartigen Organs durch die Tatsache begrenzt wäre, daß er selbst Angehöriger der Behörde, die die Datenbank führt, ist und daher weisungsgebunden wäre. Es ist allerdings denkbar, daß einzelne Betriebsordnungen im Sinne des § 9 die Namhaftmachung eines bei der Datenbank Beschäftigten vorsehen, dem die Aufsicht über die Einhaltung der Datenschutzbestimmungen obliegt.

Zu § 16:

Aus der Entscheidung für die Einrichtung einer Kollegialbehörde nach Art. 133 Z. 4 B-VG (§ 15) ergibt sich die Notwendigkeit, die Mitglieder dieser Behörde in Ausübung aller mit dieser Tätigkeit in Zusammenhang stehenden Entscheidungsvorgängen, das ist in der Vollversammlung und in den Senaten, durch eine Gesetzesbestimmung unabhängig und weisungsfrei zu stellen.

Zu § 17:

Der richterliche Einfluß auf die Entscheidungen der Datenschutzkommissionen soll durch die Wahl eines Richters zum Vorsitzenden und zum stellvertretenden Vorsitzenden zum Ausdruck kommen. Einer Beschränkung des Einflusses der Verwaltung auf die Datenschutzkommissionen entspricht auch die Bestimmung, daß die Datenschutzkommission selbst ihren Vorsitzenden wählt. Sollten der Datenschutzkommission allerdings weiterreichende Befugnisse nichtjuristischer Art zukommen (etwa im Hinblick auf eine Begutachtung neu einzurichtender Datenbanken ähnlich der schwedischen Datainspektionen), so wäre die — verfassungsrechtlich nicht notwendige — Bestellung eines Richters zum Vorsitzenden zu überdenken.

Zu § 18:

Die Mitglieder der Datenschutzkommission sollen ihr Amt nicht hauptberuflich ausüben, da an eine Heranziehung von Sachverständigen von verschiedenen Berufsgruppen der Verwaltung und der Gerichtsbarkeit, aber auch des privaten Datenverarbeitungsbereiches gedacht ist. Es wird daher davon ausgegangen, daß die Entschädigung für ihre zusätzliche Arbeit in einer Geldleistung besteht, die je nach Zahl der behandelten Fälle bzw. Teilnahme an Sitzungen über Beschwerden, an Sitzungen der Vollversammlung jährlich von der Bundesregierung (bzw. für die Landes-Datenschutzkommission von der Landesregierung) durch Verordnung festzusetzen ist. Diese Festlegung wird pauschaliert, je Fall bzw. Sitzung zu erfolgen haben. Sie kann erfolgen für das vergangene, das laufende oder das folgende Jahr und wird zweckmäßig in mehrmonatigem Abstand zur Auszahlung zu gelangen haben; mangels eines anderen Rechtszuges wird im Streitfall der Verfassungsgerichtshof gemäß Art. 137 B-VG über die Ansprüche eines Mitgliedes einer Datenschutzkommission zu entscheiden haben. Für ein allenfalls notwendiges hauptberuflich tätiges Personal der Bundes-Datenschutzkommission (Leiter des Sekretariats, Kanzleipersonal) wird im Rahmen des Dienstpostenplanes des Bundeskanzleramtes vorzusorgen sein. Wieweit dies notwendig sein wird, wird sich erst aus der Zahl und dem Umfang der durchzuführenden Verfahren ergeben.

Zu § 19:

Die Datenschutzkommissionen haben in Senaten zu je fünf Mitgliedern zu entscheiden, wobei die Zusammensetzung der Senate ad hoc für das jeweilige Verfahren durch Los bestimmt wird. Auf eine besondere Geschäftsordnung für die Datenschutzkommissionen wird anbetracht der detaillierten Regelungen des Gesetzes wohl verzichtet werden können.

Auf das Verfahren der Datenschutzkommissionen ist das AVG 1950 anzuwenden, was u. a. bedeutet, daß der belangten Stelle Parteistellung zukommt, daß die Datenschutzkommission nach Einleitung des Verfahrens nach § 20 oder § 21 von Amts wegen vorzugehen hat und daß ihr alle Beweismittelmöglichkeiten des AVG, daher auch die Einschau in der Datenbank, zustehen.

Die Bestimmungen des Abs. 5 sind denen des § 63 VwGG nachgebildet, wobei davon auszugehen sein wird, daß die Datenschutzkommission — außer bei Zurückweisung einer Beschwerde — einen Feststellungsbescheid erläßt, zu dem bei einem einer Beschwerde stattgebenden Fall eine Berichtigungspflicht (im Sinne des § 11) auferlegt werden kann. Der Adressat dieses Bescheides hat je nach den ihm möglichen Mitteln, was vom Verhältnis zwischen Datenbank und der die Datenbank führenden bzw. beaufsichtigenden Behörde abhängen wird (vgl. die Formulierungen im § 11 und im § 14), durch Weisung, durch Geltendmachung vertraglicher Mittel u. ä. den der Rechtsanschauung der Datenschutzkommission entsprechenden Zustand herzustellen. Die Datenschutzkommission kann auch eine Behörde (Gericht oder Verwaltungsbehörde) bestimmen, die den Bescheid zu vollstrecken hat.

Die Bestimmungen der Abs. 4 und 5 können als Annexmaterie (§ 1 dieses Entwurfes; Art. 11 Abs. 2 B-VG) vom Bundesgesetzgeber erlassen werden.

Zu § 20:

Die Zuständigkeit der Datenschutzkommission ist zunächst nur gegeben, wenn kein ordentliches Gericht zur Ahndung und Feststellung von Verletzungen von Bestimmungen dieses Gesetzes zuständig ist. Eine Gerichtszuständigkeit wird etwa gegeben sein, wenn in Rechtsvorschriften, die Datenbanken vorsehen, eine Zuständigkeit von Gerichten über den Inhalt der Datenbank vorgesehen ist bzw. wenn sich aus Verletzungen des Datenschutzgesetzes Schadenersatzforderungen ergeben, bei auf Grund von Verträgen nach § 14 durchgeführter Datenverarbeitung oder in den Fällen des § 18 dieses Gesetzes.

Ist bei einer anderen Verwaltungsbehörde (das wird eine Verwaltungsbehörde sein, die für die Feststellung der Daten sachlich zuständig ist) bereits ein Verfahren zur Berichtigung oder Löschung von Daten anhängig, so wird die Datenschutzkommission eine Beschwerde wegen Berichtigung zurückzuweisen haben. (Ist ihre Entscheidung über eine verlangte Berichtigung dagegen von der Entscheidung einer anderen Behörde in einem noch nicht anhängigen Verfahren abhängig, so wird die Datenschutzkommission im Rahmen ihres pflichtgemäßen Ermessens ihr Verfahren gemäß § 38 AVG zu unterbrechen haben.)

Für die Bejahung der Zuständigkeit der Datenschutzkommission ist weiters Voraussetzung, daß der Beschwerdeführer in seinen Rechten verletzt zu sein behauptet. Es ist also nicht Voraussetzung, daß er „Betroffener" im Sinne des § 2 Z. 2 ist (wenngleich dies der Regelfall sein wird). Daten, deren gesetzwidrige Weitergabe u. ä. ihn in seinen Rechten beeinträchtigt, können auch andere Personen betreffen. Als Beispiel sei hier der Fall angeführt, daß in einem Personenregister jemand als verheiratet geführt wird, obwohl er bereits geschieden ist; in diesem Fall wird die geschiedene Gattin ein Berichtigungsrecht haben, das sie selbst aber nicht unmittelbar auf Grund des § 11 beantragen kann, sondern nur durch eine auf Grund ihrer Beschwerde gefällte Entscheidung der Datenschutzkommission; ähnliche Fälle werden vorliegen für Rechtsnachfolger nach einem verstorbenen Betroffenen oder für Erziehungsberechtigte gegenüber ihren Kindern.

Die Zuständigkeit der Datenschutzkommission ist immer in erster Instanz gegeben, sei es, daß die die Datenbank führende Einrichtung einem Antrag gemäß § 10 oder § 11 nicht fristgerecht entsprochen hat, sei es, daß der Beschwerdeführer eine Verletzung anderer Bestimmungen der Abschnitte II und III behauptet (z. B. Verletzung der Datenbank-Verordnung). Es soll somit der die Datenbank führenden Stelle (die ja keine Behörde sein muß) keine Zuständigkeit für einen individuellen Bescheidabspruch gegeben werden (vgl. auch die Erläuterungen zu § 11). Diese Ausnahme vom Grundsatz der sich aus dem Verwaltungsaufbau ergebenden instanzenmäßigen Hierarchie der Behörden scheint aus mehreren Gründen gerechtfertigt: Es handelt sich um spezifische Fragen, die weniger mit der besonderen Verwaltungsmaterie, sondern hauptsächlich mit der Auslegung des Datenschutzgesetzes zusammenhängen, es handelt sich teilweise um Fragen, deren Beantwortung wesentliche Kenntnisse der Datenverarbeitung voraussetzt und deren rechtliche Beurteilung überwiegend von Fragen des Persönlichkeitsrechtes und der Privatsphäre abhängt. Da es aus der Sicht personenbezogener Daten und der möglichen Gefährdung der Privatsphäre zunächst unbeachtlich ist, ob diese Daten von einem Bundesministerium, von einem Fonds, von einem Sozialversicherungsträger u. ä. verarbeitet werden, ist es notwendig, als Entscheidungsinstanz eine einzige Behörde vorzusehen, um die Einheitlichkeit der Rechtsprechung zu gewährleisten.

Wird in einem Verwaltungsverfahren die Verletzung des DSG oder der Durchführungsverordnungen behauptet, so hat die Behörde nicht die Wahlmöglichkeit des § 38 AVG, sondern sie hat das Verfahren bis zur Entscheidung der zuständigen Datenschutzkommission zu unterbrechen und ein Verfahren bei dieser anhängig zu machen, außer es ist Gefahr im Verzug. Auch

diese Ausnahme vom AVG ist in der notwendigen Sachkenntnis und Entscheidungskonzentration begründet.

Die Bindungswirkung einer Entscheidung der sachlich zuständigen Behörde bei Berichtigungsanträgen entspricht der Bindung der die Datenbank führenden Stelle; eine Doppelgleisigkeit von Verfahren soll möglichst vermieden werden.

Ob die Bundes-Datenschutzkommission oder die Landes-Datenschutzkommission zuständig ist, ergibt sich daraus, durch welchen Rechtsträger das DSG verletzt worden sein soll (§ 3, § 4). Die Zuständigkeit der Datenschutzkommission wird wohl auch dann vorliegen, wenn etwa zwar ein Gesetz grundsätzlich eine Weitergabe im Sinne des § 7 ermöglicht, der Beschwerdeführer aber behauptet, daß die die Datenbank führende Stelle die gesetzliche Befugnis überschritten hat; es richtet sich in diesem Fall die Behauptung auf Verletzung des § 7, daß bei einer Überschreitung der weitergebenden Behörde keine gesetzliche Bestimmung, auf die verwiesen würde, vorläge.

Von einer Frist für die Einbringung einer Beschwerde wurde abgesehen, da die Unrichtigkeit von Daten ein Dauerzustand ist und der Zeitpunkt, von dem die Beschwerdefrist zu laufen beginnen soll, nicht eindeutig bestimmbar wäre.

Gegen die Beschwerde der Datenschutzkommissionen ist eine Anrufung des Verfassungsgerichtshofes ebenso wie die des Verwaltungsgerichtshofes möglich.

Zu § 21:

Datenbanken sowie die Erhebung von Daten zum Zwecke ihrer Verarbeitung in Datenbanken werden in der Regel personenbezogene Daten einer Vielzahl von Betroffenen beinhalten, wobei die Gleichartigkeit der Erhebung bzw. Verarbeitung für eine Mehrzahl von Personen fast als ein Wesenselement der maschinellen Datenverarbeitung angesehen werden kann. Der Fall, daß die Datenschutzkommission bei Durchführung eines auf Grund einer Beschwerde eingeleiteten Verfahrens zur Vermutung kommt, daß eine Verletzung von Bestimmungen des Datenschutzgesetzes oder der darauf gestützten Verordnungen auch für andere Betroffene stattgefunden hat oder stattfindet, ist somit ein durchaus wahrscheinlicher, und in diesem Fall muß der Datenschutzkommission die Möglichkeit einer amtswegigen Verfahrenseinleitung gegeben werden, um die Rechte auch von Betroffenen wahrnehmen zu können, die noch nicht die Datenschutzkommission angerufen haben oder die noch unbekannt sind. Die Voraussetzungen einer Präjudizialität für das durch Beschwerde eingeleitete Verfahren ist nicht notwendig für die Einleitung eines amtswegigen Verfahrens. Die Verwendung des Wortes „Betroffene" entspricht einem Geltungsplural, es kann auch bei Vermutung der Verletzung eines einzelnen Betroffenen ein amtswegiges Verfahren eingeleitet werden. Dem Betroffenen wird vom Entwurf ausdrücklich Parteistellung eingräumt. Auf das amtswegig eingeleitete Verfahren sind die Bestimmungen des § 19 über die Zusammensetzung der Senate und das Verfahren sowie über die Anfechtbarkeit der Bescheide der Datenschutzkommission beim Verwaltungsgerichtshof anzuwenden. Findet keine Verfahrensverbindung (§ 22) statt, so wird für jedes amtswegig eingeleitete Verfahren, d. h. für jeden einzelnen Betroffenen, ein eigener Senat einzusetzen sein.

§ 21 dient auch einer objektiven Richtigkeit der Datenbank, da es auch möglich ist, daß ein Betroffener von sich aus keine Beschwerde gegen rechtswidrig verarbeitete Daten erhebt, da der Rechtsbruch für ihn von Vorteil sein könnte. Auch in diesem Fall kann die Datenschutzkommission unter den Voraussetzungen des § 21 von sich aus das Verfahren einleiten und zur Entscheidung führen, wogegen dem Betroffenen nur die Beschwerde an den Verwaltungsgerichtshof (bzw. Verfassungsgerichtshof) wegen Verletzung des § 21 durch die Datenschutzkommission zusteht.

In der internationalen Diskussion wird eine noch weitergehende Befugnis der Datenbehörde gefordert, etwa in Richtung auf ein Einschau- und Kontrollrecht der Datenschutzbehörde in Datenbanken unabhängig von einem konkreten Verfahren (vgl. etwa Art. 16 f. des schwedischen Datenschutzgesetzes), auf ein Begutachtungsrecht für Datenbank-Betriebsordnungen und für Gesetzesbestimmungen über Datenverkehr, auf die Erteilung von Konzessionen und Ermächtigungen für die Verarbeitung bestimmter sensibler Daten. Für eine derartige Ausweitung der Zuständigkeiten der Datenschutzkommission sprechen zwar einige Argumente — wie die Notwendigkeit einer objektiven Kontrolle und Aufsicht neben der subjektiven durch die Betroffenen —, doch wäre die Einräumung anderer Zuständigkeiten als für Entscheidungen im Einzelfall für eine Behörde nach Art. 133 Z. 4 B-VG verfassungsrechtlich bedenklich und zum Teil unzweifelhaft nur durch eine Verfassungsbestimmung möglich (z. B. Antragsrecht beim Verfassungsgerichtshof auf Aufhebung einer Datenbank-Verordnung).

Zu § 22:

Da in Datenbanken in der Regel personenbezogene Daten einer Vielzahl Betroffener verarbeitet werden, ist der Fall, daß Mängel bei der Vollziehung dieses Gesetzes sich auf mehr als einen Betroffenen auswirken und von diesen durch Beschwerde (§ 20) geltend gemacht werden oder von einem Senat der Datenschutzkommission zu einer amtswegigen Verfahrenseinleitung

(§ 21) führen, nicht unwahrscheinlich. Um aber bei einer derartigen Verfahrenshäufung, die meist zu gleichartigen Untersuchungen und Entscheidungen führen wird, eine verwaltungsökonomische Verfahrensführung zu ermöglichen, sieht die Bestimmung des § 22 vor, daß gleichartige Verfahren aus Gründen der Zweckmäßigkeit (§ 39 AVG) zu einem einzigen verbunden werden können. Die Entscheidung über die Verbindung ist von der Vollversammlung zu treffen, der (neue) Senat wird durch das in § 19 vorgesehene Verfahren zusammengesetzt. Diese Verfahrensverbindung kann ab dem Zeitpunkt der Einleitung von Verfahren (Beschwerde, Beschluß einer Kommission auf Einleitung von Inzidenzverfahren) beschlossen werden, es ist dazu nicht notwendig, daß für die einzelnen Verfahren bereits Senate feststehen.

Zu § 23:

Die Öffentlichkeit ist über die Tätigkeit der Bundes-Datenschutzkommission regelmäßig zu informieren, und zwar durch Veröffentlichung ihrer Entscheidungen (zweckmäßig in einem jährlichen Sammelband) und durch einen Bericht an die Bundesregierung, der von dieser dem Nationalrat zur Kenntnis zu bringen ist. Der Bericht an die Bundesregierung sollte nicht nur die Durchführung und den Ausgang von Verfahren beinhalten, sondern auch bei einzelnen Datenbanken etwa beobachtete Unregelmäßigkeiten oder gegebene Probleme hinweisen, die einer Regelung durch den Gesetz- oder Verordnungsgeber bedürfen (vgl. § 20 VwGG und § 14 Abs. 3 VfGG).

Die Veröffentlichung der Entscheidungen der Bundes-Datenschutzkommission hat in einer den berechtigten Interessen der Betroffenen entsprechenden Weise zu erfolgen, d. h. es wird im Regelfall der Name und die Anschrift des Beschwerdeführers und anderer Personen nicht in die Veröffentlichung aufgenommen werden dürfen (wie dies auch bei den Entscheidungssammlungen der Höchstgerichte die Praxis ist).

Eine besondere Verschwiegenheitspflicht für die Mitglieder der Bundes-Datenschutzkommission braucht nicht normiert zu werden, da ihre Mitglieder, auch wenn sie nicht Beamte sind, als Angehörige eines mit Aufgaben der Bundesverwaltung betrauten Organs zur Amtsverschwiegenheit im Rahmen des Art. 20 Abs. 3 B-VG verpflichtet sind.

Die Bestimmungen des § 23 sind auch für die Landes-Datenschutzkommission anzuwenden, wobei der Bericht an die Landesregierung zu erstatten ist (vgl. § 4 Z. 4).

Zu § 24:

In den Begutachtungsverfahren zu den Vorentwürfen werden ebenso wie in der wissenschaftlichen Diskussion fast einhellig Datenschutzbestimmungen für private Datenbanken gefordert (vgl. den allgemeinen Teil der Erläuterungen). Die ausländischen Dokumente sehen für private Datenbanken teils ein Konzessionssystem vor (Schweden), teils sollen Datenschutzbeauftragte eingesetzt werden (Vorlage der deutschen Bundesregierung), teils sind materielle Beschränkungen der Datensammlung vorgesehen (Fair Credit Reporting Act der USA), wobei diese Dokumente mit den Aufgaben der Datenverarbeitung in einem Unternehmen je unterschiedliche Datenschutzbestimmungen verbinden (so die Vorlage der deutschen Bundesregierung: Datenverarbeitung nichtöffentlicher Stellen für eigene Zwecke — geschäftsmäßige Datenverarbeitung nichtöffentlicher Stellen für Dritte), somit eine Beziehung zum Gegenstand des Unternehmens herstellen.

§ 24 geht von dem auch § 2—1 des norwegischen Entwurfes innewohnenden Grundgedanken aus, daß die Ermittlung und Verarbeitung personenbezogener Daten für Private im Rahmen ihres Unternehmenszweckes frei sein soll, soweit die Intimsphäre des Betroffenen nicht berührt wird. Es wurde dabei auf den Begriff des Unternehmens zurückgegriffen, wie er in § 2 Abs. 1 des Umsatzsteuergesetzes 1972 enthalten ist („Unternehmer ist, wer eine gewerbliche oder berufliche Tätigkeit selbständig ausübt. Das Unternehmen umfaßt die gesamte gewerbliche oder berufliche Tätigkeit des Unternehmers. Gewerblich oder beruflich ist jede nachhaltige Tätigkeit zur Erzielung von Einnahmen, auch wenn die Absicht, Gewinn zu erzielen, fehlt, oder eine Personenvereinigung nur gegenüber ihren Mitgliedern tätig wird.") Es wird damit unter den Geltungsbereich des DSG fallen, wer sich in geschäftlichem Bereich betätigt, sowohl der Einzelne als auch handelsrechtliche Personengesellschaften, Genossenschaften und Kapitalgesellschaften. Dazu werden noch die Vereine dem Geltungsbereich des DSG unterworfen, sodaß infolge des Verweises auf § 3 und § 4 praktisch von allen für die Datenverarbeitung in Frage kommenden Rechtsträgern Datenschutzbestimmungen zu beachten sind.

Der Zweck des Vereines oder des Unternehmens wird sich meist aus den Statuten, aus den Eintragungen in Vereins-, Handels-, Gewerbe- und Genossenschaftsregister ergeben, wobei es der Vollziehung obliegen wird, festzustellen, wie im Einzelfall die Relation zwischen Unternehmenszweck und Umfang (gemeint ist der betroffene Personenkreis) und Art der verarbeiteten personenbezogenen Daten gestaltet werden darf. Ein Hinweis dafür kann sein, daß Daten aus der Geschäftsbeziehung zwischen Betroffenen und Unternehmen jedenfalls zulässig sein werden.

Zu § 25:

Die moderne Datenverarbeitungstechnik ermöglicht die Verbindung von an verschiedenen Orten gelegenen Anlagen zu einem einheitlichen Datenverarbeitungssystem bzw. die Verbindung von Ein- und Ausgabestationen mit einer räumlichen Zentraleinheit, in der Regel über herkömmliche Fernsprechleitungen (teleprocessing). Derartige Verbindungen sind von Staatsgrenzen unabhängig und kaum kontrollierbar, sodaß — wie ausländische Erfahrungen zeigen — die Gefahr des Ausweichens auf ausländische Datenverarbeitungsanlagen besteht, wenn die innerstaatlichen Gesetze die Verarbeitung bestimmter Daten nicht zulassen. Die zusätzlichen Kosten für die Datenfernverarbeitung stellen hier keine wesentliche Barriere dar. Die Heranziehung ausländischer Datenverarbeitungsanlagen zu einer der im § 2 Z. 3 genannten Tätigkeiten kann aus der Sicht eines österreichischen Datenschutzgesetzes in zwei Richtungen erfolgen: im Ausland gelegene Datenverarbeitungsanlagen verarbeiten Daten über Österreicher, und in Österreich gelegene Anlagen verarbeiten Daten über Ausländer. Für den öffentlichen Bereich wäre eine Datenverarbeitung im Ausland nur mit gesetzlicher Ermächtigung möglich, für den privaten Bereich sollten aber bis zum Inkrafttreten einer internationalen Konvention zum Gegenstand, wie sie vom Europarat und von der OECD vorgeschlagen wird, innerstaatlich Vorkehrungen gegen ein Umgehen des nationalen Datenschutzgesetzes durch ein Ausweichen ins Ausland getroffen werden. Bisher enthält nur das schwedische Datenschutzgesetz (Art. 11) eine Bestimmung, die eine Weitergabe personenbezogener Daten ins Ausland nur mit Zustimmung der Datenaufsichtsbehörde zuläßt.

Der Entwurf des § 25 schlägt nun vor, daß ausländische Datenverarbeitungsanlagen von Privaten nur unter den Bedingungen des § 24 zur Verarbeitung personenbezogener Daten herangezogen werden können. Das Unternehmen, das seinen Sitz in Österreich hat, wird daher nicht an einer Datenverarbeitung im Ausland gehindert, aber diese Datenverarbeitung darf hinsichtlich personenbezogener Daten nur in einer Weise erfolgen, wie sie auch in Österreich zulässig wäre. Dabei ist es unbeachtlich, ob sich die Datenbank (im Sinne des § 2 Z. 10) zur Gänze im Ausland befindet oder nur ein Teil von ihr (da auf die Datenverarbeitungsanlage abgestellt wird).

Da das DSG für die Verarbeitung personenbezogener Daten auch von Personen gelten soll, die nicht österreichische Staatsbürger sind oder die nicht ihren Wohnsitz in Österreich haben, unterliegt eine Verarbeitung personenbezogener Daten auch solcher Personen durch österreichische Unternehmen den Bedingungen des § 25, sodaß trotz Mangels einer internationalen Konvention sowohl einem Ausweichen für die Verarbeitung personenbezogener Daten nach Österreich als auch von Österreich wirksam begegnet werden könnte.

Zu § 26:

Die Einhaltung der Bestimmungen der §§ 24 und 25 ist von der Behörde zu überwachen, die die allgemeine Aufsicht (z. B. Gewerbeaufsicht, Versicherungsaufsicht, Kreditwesenaufsicht, Vereinsaufsicht, nicht aber das Arbeitsinspektorat) über den die Datenbank führenden Rechtsträger hat. Das Datenschutzgesetz ergänzt damit Bestimmungen der Wirtschaftsaufsicht (vgl. z. B. H. R. Laurer, Wirtschafts- und Steueraufsicht über Kredit- und Versicherungsunternehmungen, 1972; mehrere Beiträge in der Festschrift für K. Korinek, 1972, u. a.) und wird von den für diesen Wirtschafts- bzw. Unternehmensbereich zuständigen Aufsichtsbehörden zu vollziehen sein. Inwieweit die Aufsichtsbestimmungen allein eine Grundlage für Bescheide zur Beschränkung der Datenverarbeitung im Sinne des § 24 abgeben, kann nicht allgemein beurteilt werden (vgl. zu einzelnen Bestimmungen G. Stadler, a. a. O.). Ist für einen Unternehmer im Sinne des § 24 auf Grund wirtschaftsrechtlicher Bestimmungen nicht die Zuständigkeit einer Aufsichtsbehörde gegeben, so ist die zuständige Bezirksverwaltungsbehörde für die Aufsicht zuständig. Einem Betroffenen wird im aufsichtsbehördlichen Verfahren wohl Parteistellung zukommen. Gegen die Verfügungen dieser Aufsichtsbehörde steht der Rechtsmittelweg an die sachlich übergeordneten Behörden zu (Art. 103 Abs. 4 B-VG) sowie an den Verwaltungsgerichtshof und Verfassungsgerichtshof; von dieser Vorlage nicht gewählte Alternativen wären die Zuständigkeit der Datenschutzkommission in 2. Instanz gegen Bescheide der Aufsichtsbehörden, soweit damit eine Verletzung des DSG behauptet wird, bzw. sogar in 1. Instanz an Stelle der allgemeinen Aufsichtsbehörde.

Auf die Verpflichtung zur Namhaftmachung von Datenschutzbeauftragten in den einzelnen Betrieben, die für Datensicherung und Datenschutz verantwortlich sein sollen, wurde aus den gleichen Gründen wie für den öffentlichen Bereich (vgl. die Erläuterungen zu § 15) verzichtet (vgl. auch W. Steinmüller, a. a. O.).

Zu § 27:

Zur Wirksamkeit des Datenschutzes ist es notwendig, neben organisatorischen Vorschriften auch strafrechtliche Sanktionen für die Verletzung der Schutzvorschriften von Datenbanken mit personenbezogenen Daten vorzusehen. Da die Bestimmungen des Strafgesetzbuches (BGBl. Nr. 60/1974) nur einige Fälle des Mißbrauches von Daten unter Strafdrohung stellen (§ 121, § 122 u. a.) und die auf Grund der dienstrechtlichen Vorschriften möglichen dienst- und dis-

ziplinarrechtlichen Maßnahmen einerseits nicht auf alle mit dem Betrieb einer Datenbank befaßten Personen anwendbar sind und andererseits aus den Gefahren, die von der Verletzung der Datenschutzbestimmungen her drohen können, eine strengere Pönalisierung notwendig sein dürfte, sollen in das Datenschutzgesetz eigene Strafbestimmungen aufgenommen werden. Vergleichsweise findet sich bereits im Bundesgesetz über das Österreichische Gesundheitsinstitut (BGBl. Nr. 63/1973) eine Strafbestimmung für die unrechtmäßige Offenbarung oder Verwertung von dem Bereich der Gesundheit angehörenden Tatsachen des Privat-, Berufs- oder Familienlebens.

Im Hinblick auf die Rechtsprechung der Europäischen Kommission für Menschenrechte zu Art. 5 EMRK werden nicht Verwaltungsübertretungen, sondern gerichtliche Strafdrohungen vorgesehen.

Bestraft werden sollen nur vorsätzliche Taten, was eine gesonderte Anführung der Schuldform im DSG aber überflüssig macht (vgl. § 7 StGB 1974 i. V. m. Art. I Abs. 1 des Strafrechtsanpassungsgesetzes, BGBl. Nr. 422/1974). Die Strafbestimmung des § 27, die eine Bestrafung unabhängig davon vorsieht, ob ein konkretes Interesse an der Geheimhaltung verletzt wurde oder ob ein Schaden eingetreten ist, soll sich beziehen auf die widerrechtliche Weitergabe personenbezogener Daten aus einer Datenbank des öffentlichen Bereiches (im Sinne der §§ 3, 4) an bestimmte Personen oder an die Öffentlichkeit, auf deren Verwertung ohne besondere Weitergabe (z. B. Ausnutzung zu Drohungen).

In Anlehnung an den Wortlaut des Art. 20 Abs. 3 B-VG soll der Mißbrauch personenbezogener Daten für jedermann strafbar sein, soweit er diese Daten ausschließlich kraft seiner Beschäftigung mit der Datenverarbeitung zur Kenntnis erhalten hat. Die Bestimmung geht somit über den von den zur Wahrung des Amtsgeheimnisses erfaßten Personenkreis hinaus und betrifft auch Personen, die infolge einer Tätigkeit auf Grund eines Werkvertrages bei einer derartigen Datenbank Einsicht nehmen konnten, sowie Personen, die mit Servicediensten an einer EDV-Anlage, die zu einer Datenbank im Sinne des § 2 Z. 10 gehört, beschäftigt sind oder waren. Ebenso wie die Strafbestimmungen des § 29 ist es für die Bestrafung unerheblich, ob der Täter im Zeitpunkt der Tat noch bei der Datenbank beschäftigt ist, entscheidend ist nur die Beziehung zwischen der Beschäftigung mit Datenverarbeitung in einer Datenbank und Kenntnisnahme der geschützten Daten.

Zu § 28:

Diese Bestimmung soll die Offenbarung oder Verwertung von in Datenbanken verarbeiteten personenbezogenen Daten pönalisieren, soweit diese Handlungen geeignet sind, berechtigte Interessen — was im Hinblick auf Art. 8 EMRK sowie auf allfällige andere gesetzliche Bestimmungen zu beurteilen sein wird — des Betroffenen zu verletzen. Anbetracht des Verfassungssatzes des Art. 8 EMRK erscheint es rechtspolitisch gerechtfertigt, alle personenbezogenen Daten wenigstens in vergleichbarer Weise wie Geschäfts- oder Betriebsgeheimnisse zu schützen. Die Bestimmung ist nachgebildet dem § 122 des StGB 1974 (vgl. daher auch die Erläuterungen zu § 127 der Regierungsvorlage eines Strafgesetzbuchs, 30 der Beilagen, St. Prot. NR, XIII. GP vom 16. November 1971), stellt aber nicht darauf ab, daß der Täter durch Gesetz verpflichtet ist, das Geheimnis zu wahren. Ein Rechtfertigungsgrund für den Täter wird nur vorliegen, wenn das Veröffentlichungsinteresse jenes Interesse überwiegt, das der Betroffene an der Geheimhaltung hat. Das Offenbaren besteht im Mitteilen der geheimzuhaltenden Daten an einen Dritten, dem jene Daten entweder noch neu oder zumindest nicht sicher bekannt sind; auf die Art der Offenbarung kommt es nicht an. Unter Verwertung ist jedes Ausnützen des Geheimnisses zu verstehen, auch wenn der Täter es nicht dritten Personen mitteilt.

Der Personenkreis, auf den diese Strafbestimmung anzuwenden sein wird, ist das dauernd oder vorübergehend in einer (privaten) Datenbank tätige Personal, soweit dieses mit Datenverarbeitung beschäftigt ist. (Datenerfasser, Programmierer, Operatoren, Systemanalytiker, Servicetechniker u. ä.). Die Tat soll nur auf Verlangen des Betroffenen (= Verletzten) verfolgt werden (Privatanklagedelikt).

Zu § 29:

Diese Bestimmung wendet sich gegen das Offenbaren oder Verwerten (vgl. die Erläuterungen zu § 28) von personenbezogenen Daten, die unbefugt aus einer (öffentlichen oder privaten) Datenbank verschafft wurden, soweit dies berechtigte Interessen des Betroffenen (Verletzten) verletzt. Der Täterkreis ist somit ein gegenüber § 28 weiterer und von der Beschäftigung in einer Datenbank unabhängig. Wurden die Daten aus einer privaten Datenbank verschafft, liegt ein Privatanklagedelikt vor, ansonsten ein Ermächtigungsdelikt. Verschaffung aus einer Datenbank wird auch vorliegen, wenn die Daten einem Datenträger entnommen werden, der im Zeitpunkt der Tat nicht mit der maschinellen Einrichtung der Datenbank verbunden ist (z. B. Lochkarten; vgl. die Definition im § 2 Z. 10).

Zu § 30:

Für das Inkrafttreten dieses Bundesgesetzes ist zunächst der 1. Jänner 1977 vorgesehen. Zwischen Beschluß des Gesetzes und Inkrafttreten

wird eine mehrmonatige Legisvakanz notwendig sein.

Die Anwendung des Datenschutzgesetzes und insbesondere der Datenbank-Verordnung wird für einzelne Datenbanken einer Reihe von Maßnahmen administrativer und programmtechnischer Art, allenfalls auch eine Erweiterung der hardware oder eine geänderte bauliche Ausstattung notwendig machen, was eine längere Planungs- und Durchführungszeit beansprucht. Die Möglichkeit eines frühzeitigen Erlassens der Datenbank-Verordnungen ist daher zweckdienlich, da sich aus ihnen die im einzelnen notwendigen Maßnahmen erkennen lassen werden (Abs. 2).

Für Datenbanken, die im Zeitpunkt des Inkrafttretens des Gesetzes bereits in Tätigkeit sind, wird als Übergangszeitpunkt für die volle Anwendung des DSG der 1. Jänner 1978 vorgesehen, um einen aus Kosten- und Verwaltungsgründen möglicherweise notwendigen Übergangszeitraum vorzusehen.

Zu § 31:

§ 31 enthält eine dem der Gemeinde von Verfassungs wegen zugesicherten eigenen Wirkungsbereich entsprechende Bestimmung. Die Gemeinde wird daher, soweit sie organisatorisch selbständige Datenbanken führt, diese Führung auch im Hinblick der Bestimmungen des DSG im eigenen Wirkungsbereich wahrzunehmen haben, soweit sie die Daten überwiegend für ihren eigenen Wirkungskreis verarbeitet. In diesen Fällen wird die Gemeinde etwa über einen Berichtigungsanspruch gemäß § 11 abzusprechen haben. Gegen die Entscheidung der Gemeinde, die im Sinne der §§ 10 und 11 nicht bescheidmäßig zu erfolgen hat, wird keine Vorstellung (Art. 119 a Abs. 5 B-VG) zu erheben sein, sondern Beschwerde an die Landes-Datenschutzkommission (§ 20 i. V. m. § 4 Z. 6).

Zu § 32:

Diese Bestimmung enthält eine den Bestimmungen des Bundesministeriengesetzes 1973 entsprechende Vollzugsklausel und berücksichtigt auch die Vollziehung des Gesetzes durch die Länder (vgl. § 4).

3. Eine Textgegenüberstellung ist mangels geltender Vorschriften nicht möglich.