

Gesetzentwurf **der Bundesregierung**

Entwurf eines Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundes-Datenschutzgesetz – BDSG)

A. Zielsetzung

Die Information erlangt in unserer technisierten Welt immer größere Bedeutung. Die technischen Hilfsmittel für die schnelle und umfassende Bereitstellung sind vorhanden und werden ständig fortentwickelt. Das Informationsbedürfnis in allen Bereichen macht indessen auch vor der Privatsphäre des Menschen nicht Halt; in jeder denkbaren Eigenschaft werden Informationen von ihm und über ihn benötigt. Der dem Bürger vom Grundgesetz gewährte Freiheitsraum, die unantastbare Sphäre privater Lebensgestaltung drohen enger zu werden. Dieser sich anbahnenden Entwicklung gilt es durch ein umfassendes Datenschutzgesetz zu steuern. Das geltende Recht, das von einer Zersplitterung in viele, aufeinander nicht abgestimmte einschlägige Einzelvorschriften gekennzeichnet ist, wird den Anforderungen eines modernen Datenschutzes nicht gerecht.

B. Lösung

Der Entwurf eines Bundes-Datenschutzgesetzes strebt eine grundlegende Neuordnung des Rechts des Schutzes der Privatsphäre vor Mißbräuchen bei der Datenverarbeitung (Datenschutzrecht) auf Bundesebene an. Er versucht diese Problematik umfassend zu lösen, also in allen schutzrelevanten Bereichen des öffentlichen und des privaten Lebens und ohne Rücksicht auf die bei der Datenverarbeitung angewendeten Methoden. Dies geschieht im Prinzip in der Weise, daß der Umgang mit personenbezogenen Daten in den besonders schutzbedürftigen Phasen der Datenverarbeitung, nämlich dem Einspeichern, Weitergeben, Verändern und Löschen der Daten geregelt wird. Außerdem werden dem betroffenen Bürger Abwehrrechte gewährt, im wesentlichen das Recht auf Auskunft über die zu seiner Person gespeicherten Daten, ein Anspruch auf Berichtigung unzutreffend gespeicherter Daten und unter bestimmten

Voraussetzungen ein Anspruch auf Sperrung bzw. Löschung ihn betreffender Daten. Vorschriften über das Verfahren und Kontrollmaßnahmen sowie Bußgeld- und Strafvorschriften ergänzen diese Regelungen. Die Errichtung einer neuen zentralen Überwachungsinstitution ist nicht vorgesehen.

C. Alternativen

keine

D. Kosten

Ein Großteil der in diesem Entwurf vorgesehenen Schutzmaßnahmen muß aus anderen Gründen, insbesondere nach den Grundsätzen ordnungsgemäßer Datenverarbeitung einschließlich der Datensicherung ohnehin erbracht werden. Im übrigen wird die Ausführung des Gesetzes den Bund mit auf jährlich etwa 1 Million DM geschätzten Kosten belasten, die im Rahmen des durch die derzeitige Finanzplanung geltenden Plafonds aufgefangen werden. Die vom Entwurf bei Ländern und Gemeinden sowie bei den betroffenen nicht-öffentlichen Stellen verursachten Kosten sind noch nicht bezifferbar. Auswirkungen auf das allgemeine Verbraucherpreisniveau sind nicht, auf Einzelpreise kaum zu erwarten.

Bundesrepublik Deutschland
Der Bundeskanzler

I/4 (I/3) – 400 00 – Da 3/73

Bonn, den 20. September 1973

An den Präsidenten
des Deutschen Bundestages

Hiermit übersende ich den von der Bundesregierung beschlossenen Entwurf eines Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundes-Datenschutzgesetz – BDSG) mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlußfassung des Deutschen Bundestages herbeizuführen.

Federführend ist der Bundesminister des Innern.

Der Bundesrat hat in seiner 396. Sitzung am 6. Juli 1973 gemäß Artikel 76 Abs. 2 des Grundgesetzes beschlossen, zu dem Gesetzentwurf wie aus der Anlage 2 ersichtlich Stellung zu nehmen.

Die Auffassung der Bundesregierung zu der Stellungnahme des Bundesrates ist in der Gegenäußerung (Anlage 3) dargelegt.

Brandt

Anlage 1

Entwurf eines Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundes-Datenschutzgesetz – BDSG)**Erster Abschnitt – Allgemeine Vorschriften**

- § 1 Zweck des Gesetzes
- § 2 Gegenstand des Datenschutzes
- § 3 Begriffsbestimmungen
- § 4 Technische und organisatorische Maßnahmen des Datenschutzes

Zweiter Abschnitt – Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen

- § 5 Anwendungsbereich
- § 6 Datenspeicherung
- § 7 Datenaustausch innerhalb des öffentlichen Bereichs
- § 8 Datenweitergabe an Dritte
- § 9 Datenveränderung
- § 10 Veröffentlichung über die gespeicherten Daten
- § 11 Auskunftserteilung
- § 12 Berichtigung, Löschung und Sperrung von Daten
- § 13 Verarbeitung personenbezogener Daten im Auftrag anderer Behörden und sonstiger Stellen
- § 14 Durchführung des Datenschutzes in der Bundesverwaltung
- § 15 Allgemeine Verwaltungsvorschriften

Dritter Abschnitt – Datenverarbeitung nicht-öffentlicher Stellen für eigene Zwecke

- § 16 Anwendungsbereich
- § 17 Datenspeicherung
- § 18 Datenweitergabe
- § 19 Datenveränderung
- § 20 Auskunftserteilung
- § 21 Berichtigung, Löschung und Sperrung von Daten
- § 22 Durchführung des Datenschutzes

Vierter Abschnitt – Geschäftsmäßige Datenverarbeitung nicht-öffentlicher Stellen für Dritte

- § 23 Anwendungsbereich
- § 24 Datenspeicherung und -weitergabe
- § 25 Datenveränderung
- § 26 Auskunftserteilung
- § 27 Berichtigung, Löschung und Sperrung von Daten
- § 28 Verarbeitung personenbezogener Daten zum Zwecke der Weitergabe in anonymisierter Form
- § 29 Verarbeitung personenbezogener Daten im Auftrag Dritter
- § 30 Meldepflichten
- § 31 Aufsichtsbehörde

Fünfter Abschnitt – Straf- und Bußgeldvorschriften

- § 32 Straftaten
- § 33 Verletzung der Geheimhaltungspflicht
- § 34 Ordnungswidrigkeiten

Sechster Abschnitt – Übergangs- und Schlußvorschriften

- § 35 Übergangsvorschriften
- § 36 Anwendung des Verwaltungsverfahrensgesetzes
- § 37 Weitergehende Datenschutzvorschriften
- § 38 Berlin-Klausel
- § 39 Inkrafttreten

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

ERSTER ABSCHNITT

Allgemeine Vorschriften

§ 1

Zweck des Gesetzes

Zweck dieses Gesetzes ist es, personenbezogene Daten vor Mißbrauch bei der Datenverarbeitung zu schützen und dadurch der Beeinträchtigung schutzwürdiger Belange der Betroffenen entgegenzuwirken.

§ 2

Gegenstand des Datenschutzes

(1) Dieses Gesetz schützt personenbezogene Daten, soweit sie

1. von Behörden oder sonstigen öffentlichen Stellen (§ 5),
2. von Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts für eigene Zwecke (§ 16),
3. von Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts geschäftsmäßig für Dritte (§ 23)

in Dateien gespeichert und sonst verarbeitet werden, es sei denn, daß die personenbezogenen Daten nicht für die Weitergabe an Dritte bestimmt sind. Sollen die personenbezogenen Daten abweichend von ihrer in Satz 1 letztem Halbsatz genannten Zweckbestimmung an Dritte weitergegeben werden, gelten die einschlägigen Vorschriften des Gesetzes.

(2) Dieses Gesetz schützt nicht personenbezogene Daten, soweit sie unmittelbar aus allgemein zugänglichen Quellen entnommen worden sind. Es schützt ferner nicht personenbezogene Daten, soweit sie durch natürliche oder juristische Personen, Gesellschaften oder andere Personenvereinigungen, die Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films sind oder betreiben, zu publizistischen Zwecken in Dateien gespeichert und weitergegeben werden.

(3) Die Verarbeitung personenbezogener Daten, die von diesem Gesetz geschützt werden, ist nur zulässig, wenn

1. der Betroffene zugestimmt hat oder
2. dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt. Die Zustimmung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist; wird die Zustimmung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf besonders hinzuweisen.

§ 3

Begriffsbestimmungen

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

(2) Im Sinne dieses Gesetzes ist

1. Datenverarbeitung (Verarbeitung von Daten) das Speichern, Verändern, Weitergeben oder Löschen von Daten,
2. Speichern (Speicherung) das Festhalten von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verwendung,
3. Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter Daten,
4. Weitergeben (Weitergabe) das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an Personen oder Stellen außerhalb der speichernden Stelle (Dritte),
5. Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten,

ungeachtet der dabei angewendeten Verfahren.

(3) Im Sinne dieses Gesetzes ist eine Datei eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet, nach anderen bestimmten Merkmalen umgeordnet und ausgewertet werden kann, ungeachtet der dabei angewendeten Verfahren. Nicht hierzu gehören insbesondere Akten, Aktensammlungen und Bücher.

§ 4

Technische und organisatorische Maßnahmen des Datenschutzes

(1) Wer im Rahmen des § 2 Abs. 1 personenbezogene Daten verarbeitet, hat die erforderlichen und zumutbaren technischen und organisatorischen Maßnahmen gegen Mißbräuche bei der Datenverarbeitung, insbesondere gegen unzulässiges Abrufen, Weitergeben, Verändern und Löschen zu treffen. Zumutbar sind nur Maßnahmen, deren Schutzwirkung in einem angemessenen Verhältnis zu dem Aufwand steht, den sie verursachen.

(2) Die Bundesregierung wird ermächtigt, durch Rechtsverordnung mit Zustimmung des Bundesrates Grundsätze über Maßnahmen im Sinne von Absatz 1, ihren Einsatz und ihre Durchführung zu erlassen. In der Rechtsverordnung können auch bestimmte Maßnahmen im Sinne von Absatz 1 vorgeschrieben sowie das Nähere zu § 7 Abs. 3, § 8 Abs. 4, § 9 Abs. 2, § 13 Abs. 2, § 18 Satz 4, § 19 Satz 3, § 24 Abs. 2 Satz 4, § 25 Satz 3, § 28 Abs. 2, § 29 Abs. 2 geregelt werden. Die Bundesregierung kann die Ermächtigung nach Satz 2 für den Anwendungsbereich der in § 5 Abs. 1 Satz 2 genannten Behörden und sonstigen Stellen durch Rechtsverordnung mit Zustimmung des Bundesrates auf die Landesregierung übertragen.

ZWEITER ABSCHNITT

Datenverarbeitung der Behörden
und sonstigen öffentlichen Stellen

§ 5**Anwendungsbereich**

(1) Die Vorschriften dieses Abschnittes gelten für Behörden und sonstige Stellen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie für Vereinigungen solcher Körperschaften, Anstalten und Stiftungen. Sie gelten mit Ausnahme der §§ 14 und 15 auch für Behörden und sonstige Stellen der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen, soweit sie Bundesrecht ausführen oder soweit es sich dabei um Gerichte oder Behörden der Staatsanwaltschaft handelt.

(2) Abweichend von Absatz 1 gelten für öffentlich-rechtliche Versicherungsunternehmen, die am Wettbewerb teilnehmen, und für öffentlich-rechtliche Kreditinstitute von den Vorschriften dieses Abschnittes nur die §§ 13 bis 15.

(3) Die Vorschriften dieses Abschnittes gelten für die in Absatz 1 genannten Behörden und sonstigen Stellen auch insoweit, als das Speichern in Dateien und die sonstige Verarbeitung personenbezogener Daten in deren Auftrag durch andere Stellen betrieben werden. Sie gelten mit Ausnahme der §§ 13 bis 15 nicht für Behörden und sonstige Stellen, soweit sie in den Fällen des Satzes 1 im Auftrag tätig werden. § 13 gilt auch für juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, soweit diese Personen oder Personenvereinigungen in den Fällen des Satzes 1 im Auftrag tätig werden.

(4) Abweichend von Absatz 1 gelten anstelle der §§ 6 bis 12 die §§ 17 bis 21 entsprechend, soweit die Datenverarbeitung frühere, bestehende oder zukünftige dienst- und arbeitsrechtliche Rechtsverhältnisse betrifft.

(5) Behörde im Sinne dieses Gesetzes ist jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt.

§ 6**Datenspeicherung**

Das Speichern personenbezogener Daten ist im Rahmen rechtmäßiger Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben zulässig.

§ 7**Datenaustausch
innerhalb des öffentlichen Bereichs**

(1) Die Weitergabe personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis (§ 37 Satz 2 Nr. 1, Satz 3) unterliegen und der weitergebenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht weitergegeben worden sind, an Behörden und sonstige öffentliche Stellen ist zulässig, wenn der Empfänger sie zur Erfüllung des gleichen Zweckes benötigt, zu dem sie die weitergebende Stelle erhalten hat. Die Weitergabe anderer personenbezogener Daten ist im Rahmen rechtmäßiger Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben zulässig.

(2) Die Weitergabe personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgemeinschaften ist wie die Datenweitergabe an Behörden und sonstige öffentliche Stellen zulässig, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

(3) Können personenbezogene Daten durch selbsttätige Einrichtungen weitergegeben werden, so sind Vorkehrungen zu treffen, daß sie nur in dem zulässigen Umfang selbsttätig weitergegeben, insbesondere nicht durch Unbefugte abgerufen werden können. Durch Dokumentation der Datenverarbeitungsprogramme und erforderlichenfalls durch weitere Unterlagen ist nachzuweisen, an welche Stellen und in welchem Umfang Daten weitergegeben werden. Werden Daten selbsttätig abgerufen, ist ferner ein Protokoll zu führen, das die abrufende Stelle sowie Art und Zeitpunkt des Abrufs ausweist.

§ 8**Datenweitergabe an Dritte**

(1) Die Weitergabe personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis (§ 37 Satz 2 Nr. 1, Satz 3) unterliegen und der weitergebenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht weitergegeben worden sind, an andere Personen als den Betroffenen und an andere Stellen als die in § 7 Abs. 1 und 2 bezeichneten ist zulässig, wenn die gleichen Voraussetzungen gegeben sind, unter denen sie die zur Verschwiegenheit verpflichtete Person weitergeben dürfte. Die Weitergabe anderer personenbezogener Daten ist zulässig im Rahmen rechtmäßiger Erfüllung der in der Zuständigkeit der weitergebenden Stelle liegenden Aufgaben oder soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der weiterzugebenden Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Für die Weitergabe an Behörden und sonstige Stellen außerhalb des Geltungsbereichs dieses

Gesetzes sowie an über- und zwischenstaatliche Stellen finden die Sätze 1 und 2 nach Maßgabe der für diese Weitergabe geltenden Gesetze und Vereinbarungen Anwendung.

(2) Abweichend von Absatz 1 ist die Weitergabe folgender Daten (freie Daten) zulässig:

1. Namen,
2. Titel, akademische Grade,
3. Geburtsdatum,
4. Beruf, Branchen- oder Geschäftsbezeichnung,
5. Anschrift,
6. Rufnummer.

(3) Die Weitergabe personenbezogener Daten nach den Absätzen 1 und 2 ist nicht zulässig, wenn Tatsachen die Annahme rechtfertigen, daß dem Betroffenen oder einer anderen Person aus der Datenweitergabe eine Gefahr für Leben, Gesundheit oder die persönliche Freiheit erwachsen kann.

(4) Für die Weitergabe personenbezogener Daten durch selbsttätige Einrichtungen gilt § 7 Abs. 3 entsprechend.

§ 9

Datenveränderung

(1) Das Verändern personenbezogener Daten ist zulässig im Rahmen rechtmäßiger Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben. Die Berichtigungspflicht nach § 12 Abs. 1 bleibt unberührt.

(2) Bei automatischer Datenverarbeitung sind Vorkehrungen zu treffen, daß die Daten nur in dem zulässigen Umfang verändert werden können.

§ 10

Veröffentlichung über die gespeicherten Daten

Die speichernde Stelle veröffentlicht die Art und den Umfang der von ihr gespeicherten personenbezogenen Daten sowie den betroffenen Personenkreis unverzüglich nach der ersten Einspeicherung in dem für ihren Bereich bestehenden Veröffentlichungsblatt für amtliche Bekanntmachungen. Satz 1 gilt nicht für die Ämter für Verfassungsschutz, den Bundesnachrichtendienst, den militärischen Abschirmdienst, das Bundeskriminalamt, die Behörden der Staatsanwaltschaft und der Polizei sowie für Bundes- und Landesfinanzbehörden, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Reichsabgabenordnung zur Überwachung und Prüfung in Dateien speichern oder sonst verarbeiten.

§ 11

Auskunftserteilung

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

(2) Absatz 1 gilt nicht für die in § 10 Satz 2 genannten Behörden.

(3) Eine Verpflichtung zur Auskunftserteilung besteht nicht, soweit

1. die Auskunft die rechtmäßige Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft für die öffentliche Sicherheit oder Ordnung oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen einer dritten Person, geheimgehalten werden müssen,
4. die Auskunft sich auf die Weitergabe personenbezogener Daten an die in § 10 Satz 2 genannten Behörden bezieht.

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

§ 12

Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird die Richtigkeit personenbezogener Daten vom Betroffenen bestritten und läßt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, so ist den Daten bei künftigen Weitergaben ein entsprechender Hinweis beizufügen.

(2) Personenbezogene Daten können gelöscht werden, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und durch die Löschung schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden; sie sind zu löschen, wenn ihre Speicherung unzulässig war.

(3) Personenbezogene Daten sind zu sperren, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und durch das Unterlassen der Sperrung schutzwürdige Belange des Betroffenen beeinträchtigt werden würden. Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr verarbeitet, insbesondere weitergegeben, oder sonst genutzt werden, es sei denn, daß die Nutzung zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen geboten ist oder der Betroffene der Nutzung zugestimmt hat.

§ 13

Verarbeitung personenbezogener Daten im Auftrag anderer Behörden und sonstiger Stellen

(1) Den in § 5 Abs. 3 Sätze 2 und 3 genannten Behörden und sonstigen Stellen sind Weitergabe, Veränderung und Löschung personenbezogener Daten nur mit Zustimmung der Behörden oder sonstigen Stellen gestattet, in deren Auftrag die Daten in Dateien gespeichert und sonst verarbeitet werden.

(2) Bei automatischer Datenverarbeitung sind Vorkehrungen zu treffen, daß die Daten nur in dem zulässigen Umfang weitergegeben, verändert und gelöscht und nicht durch Unbefugte abgerufen werden können.

§ 14

Durchführung des Datenschutzes in der Bundesverwaltung

Die obersten Bundesbehörden, der Vorstand der Deutschen Bundesbahn sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von einer obersten Bundesbehörde lediglich Rechtsaufsicht ausgeübt wird, haben jeweils für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Sie haben insbesondere dafür zu sorgen, daß

1. eine Übersicht über die Art der gespeicherten personenbezogenen Daten und über die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, sowie über deren regelmäßige Empfänger geführt und

2. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird.

§ 15

Allgemeine Verwaltungsvorschriften

Die obersten Bundesbehörden und der Vorstand der Deutschen Bundesbahn erlassen jeweils für ihren Geschäftsbereich allgemeine Verwaltungsvorschriften, die die Ausführung dieses Gesetzes, bezogen auf die besonderen Verhältnisse in dem jeweiligen Geschäftsbereich und die sich daraus ergebenden besonderen Erfordernisse für den Datenschutz, regeln.

DRITTER ABSCHNITT

Datenverarbeitung nicht-öffentlicher Stellen für eigene Zwecke

§ 16

Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für natürliche oder juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie personenbezogene Daten als Hilfsmittel für die Erfüllung ihrer Geschäftszwecke oder Ziele in Dateien speichern und sonst verarbeiten. Sie gelten, mit Ausnahme von § 22, nach Maßgabe von Satz 1 auch für öffentlich-rechtliche Versicherungsunternehmen, die am Wettbewerb teilnehmen, und für öffentlich-rechtliche Kreditinstitute.

(2) Die Vorschriften dieses Abschnittes gelten für die in Absatz 1 genannten Personen, Gesellschaften und andere Personenvereinigungen auch insoweit, als das Speichern in Dateien und die sonstige Verarbeitung personenbezogener Daten in deren Auftrag durch andere Stellen betrieben werden.

(3) Die Vorschriften dieses Abschnittes gelten nicht für die in Absatz 1 Satz 1 genannten Personen, Gesellschaften und andere Personenvereinigungen, die Aufgaben der öffentlichen Verwaltung wahrnehmen.

§ 17

Datenspeicherung

Das Speichern personenbezogener Daten ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen oder soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

§ 18

Datenweitergabe

Die Weitergabe personenbezogener Daten, die einem Berufs- oder besonderem Amtsgeheimnis (§ 37 Satz 2 Nr. 1, Satz 3) unterliegen und der weitergebenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht weitergegeben worden sind, ist zulässig, wenn die gleichen Voraussetzungen gegeben sind, unter denen sie die zur Verschwiegenheit verpflichtete Person weitergeben dürfte. Die Weitergabe anderer personenbezogener Daten ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen oder soweit es zur Wahrung berechtigter Interessen der weitergebenden Stelle oder eines Dritten erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Die Weitergabe von freien Daten (§ 8 Abs. 2) ist abweichend von den Sätzen 1 und 2 stets zulässig. § 7 Abs. 3 gilt entsprechend.

§ 19

Datenveränderung

Das Verändern personenbezogener Daten ist zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen oder soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Die Berichtigungspflicht nach § 21 Abs. 1 bleibt unberührt. § 9 Abs. 2 gilt entsprechend.

§ 20

Auskunftserteilung

(1) Werden erstmals zur Person des Betroffenen Daten gespeichert, ist er darüber zu benachrichtigen, es sei denn, daß er auf andere Weise Kenntnis von der Speicherung erlangt hat.

(2) Der Betroffene kann Auskunft über die zu seiner Person gespeicherten Daten verlangen. Er hat die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher zu bezeichnen. Die Auskunft wird schriftlich erteilt, soweit nicht wegen besonderer Umstände eine andere Form der Auskunftserteilung angemessen ist.

(3) Für die Auskunft kann ein Entgelt verlangt werden, das über die durch die Auskunftserteilung entstandenen unmittelbaren Kosten nicht hinausgehen darf. Ein Entgelt kann nicht verlangt werden, wenn die Auskunft ergeben hat, daß die personenbezogenen Daten zu berichtigen oder unter der Voraussetzung des § 21 Abs. 2 Satz 2 zu löschen sind.

(4) Die Absätze 1 und 2 gelten nicht, soweit

1. das Bekanntwerden personenbezogener Daten die Geschäftszwecke oder Ziele der speichernden Stelle erheblich gefährden würde und überwiegende berechnete Interessen des Betroffenen nicht entgegenstehen,
2. das Bekanntwerden der personenbezogenen Daten für die öffentliche Sicherheit oder Ordnung oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
3. die personenbezogenen Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der überwiegenden berechtigten Interessen einer dritten Person, geheimgehalten werden müssen.

§ 21

Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird die Richtigkeit personenbezogener Daten vom Betroffenen bestritten und läßt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, so ist den Daten bei künftigen Weitergaben ein entsprechender Hinweis beizufügen.

(2) Personenbezogene Daten können gelöscht werden, wenn ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist und durch die Löschung schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Sie sind zu löschen, wenn ihre Speicherung unzulässig war.

(3) Personenbezogene Daten sind zu sperren, wenn ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist und der Betroffene es verlangt. Die Vorschriften über das Verfahren und die Rechtsfolgen der Sperrung in § 12 Abs. 3 Satz 2 gelten entsprechend.

§ 22

Durchführung des Datenschutzes

(1) Die in § 16 Abs. 1 und 2 genannten Personen, Gesellschaften und anderen Personenvereinigungen, die die Datenverarbeitung automatisch betreiben und hierbei in der Regel mindestens fünf Arbeitnehmer ständig beschäftigen, haben spätestens binnen eines Monats nach Aufnahme ihrer Tätigkeit einen Beauftragten für den Datenschutz zu berufen, der die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen hat. Der Beauftragte für den Datenschutz ist insoweit dem Inhaber, dem Vorstand, dem Geschäftsführer oder dem sonstigen gesetzlich oder verfassungsmäßig berufenen Leiter der Stelle unmittelbar unterstellt. Die Sätze 1 und 2 gelten auch, wenn die Datenverarbeitung nicht automatisch betrieben wird und soweit hierbei in der Regel mindestens zwanzig Arbeitnehmer ständig beschäftigt sind.

(2) Zu den Aufgaben des Beauftragten für den Datenschutz gehört es insbesondere,

1. eine Übersicht über die Art der gespeicherten personenbezogenen Daten und über die Geschäftszwecke und Ziele, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, sowie über deren regelmäßige Empfänger zu führen,
2. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen,
3. die bei der Datenverarbeitung tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, bezogen auf die besonderen Verhältnisse in diesem Geschäftsbereich und die sich daraus ergebenden besonderen Erfordernisse für den Datenschutz, vertraut zu machen,
4. bei der Auswahl der in der Datenverarbeitung tätigen Personen beratend mitzuwirken.

VIERTER ABSCHNITT

Geschäftsmäßige Datenverarbeitung
nicht-öffentlicher Stellen für Dritte

§ 23

Anwendungsbereich

Für natürliche oder juristische Personen, Gesellschaften oder andere Personenvereinigungen des privaten Rechts gelten

1. die §§ 24 bis 27, 30 und 31 dieses Abschnittes, soweit diese Stellen geschäftsmäßig personenbezogene Daten zum Zweck der Weitergabe in Dateien speichern und weitergeben; dabei ist es unerheblich, ob die Daten vor der Weitergabe verändert oder sonst verarbeitet werden,
2. die §§ 28, 30 und 31, soweit diese Stellen geschäftsmäßig personenbezogene Daten zum Zweck der Veränderung in Dateien speichern, sie derart verändern, daß diese Daten sich weder auf eine bestimmte Person beziehen noch eine solche erkennen lassen (anonymisieren), und sie in dieser Form weitergeben,
3. die §§ 29 bis 31, soweit diese Stellen geschäftsmäßig personenbezogene Daten im Auftrag Dritter zum Zweck der Datenverarbeitung in Dateien speichern und sonst verarbeiten; ausgenommen sind juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, soweit diese Personen oder Personenvereinigungen im Auftrag von Behörden oder sonstigen öffentlichen Stellen tätig werden.

§ 24

Datenspeicherung und -weitergabe

(1) Das Speichern personenbezogener Daten ist zulässig, soweit kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

(2) Die Weitergabe von personenbezogenen Daten ist zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat. Ein berechtigtes Interesse kann insbesondere im Zusammenhang mit einem Kredit-, Versicherungs- oder Dienstvertrag gegeben sein. Die Gründe für das Vorliegen eines berechtigten Interesses und die Mittel für ihre glaubhafte Darlegung sind aufzuzeichnen. § 7 Abs. 3 gilt entsprechend.

(3) Abweichend von Absatz 2 Satz 1 ist die Weitergabe zulässig, wenn sie sich auf freie Daten (§ 8 Abs. 2) sowie auf eine Angabe über die Zugehörigkeit des Betroffenen zu einer Personengruppe beschränkt und kein Grund zur Annahme besteht, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

§ 25

Datenveränderung

Das Verändern personenbezogener Daten ist zulässig, soweit dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Die Berichtspflicht nach § 27 Abs. 1 bleibt unberührt. § 9 Abs. 2 gilt entsprechend.

§ 26

Auskunftserteilung

(1) Werden erstmals zur Person des Betroffenen gespeicherte Daten weitergegeben, ist er über die Speicherung zu benachrichtigen, es sei denn, daß er auf andere Weise von der Speicherung Kenntnis erlangt hat. Satz 1 gilt nicht für Weitergaben nach § 24 Abs. 3.

(2) Der Betroffene kann Auskunft über die zu seiner Person gespeicherten Daten verlangen. Die Auskunft wird schriftlich erteilt, soweit nicht wegen besonderer Umstände eine andere Form der Auskunftserteilung angemessen ist.

(3) Für die Auskunft kann ein Entgelt verlangt werden, das über die durch die Auskunftserteilung entstandenen unmittelbaren Kosten nicht hinausgehen darf. Ein Entgelt kann nicht verlangt werden, wenn die Auskunft ergeben hat, daß die personenbezogenen Daten zu berichtigen oder unter der Voraussetzung des § 27 Abs. 3 Satz 2 zu löschen sind.

(4) Die Absätze 1 und 2 gelten nicht, soweit das Bekanntwerden der personenbezogenen Daten für die öffentliche Sicherheit oder Ordnung oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten oder überwiegende berechnete Interessen einer dritten Person schädigen würde.

§ 27

**Berichtigung, Löschung und Sperrung
von Daten**

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird die Richtigkeit personenbezogener Daten vom Betroffenen bestritten und läßt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, so ist den Daten ein entsprechender Hinweis beizufügen. In den in Satz 2 genannten Fällen kann der Betroffene auch verlangen, daß den Daten seine Gegendarstellung beigefügt wird.

(2) Berichtigung, Hinweis und Gegendarstellung sind den bisherigen Empfängern der betreffenden Daten zur Kenntnis zu bringen. Daten, denen ein Hinweis oder eine Gegendarstellung beigefügt ist, dürfen ohne Hinweis oder Gegendarstellung nicht weitergegeben werden.

(3) Personenbezogene Daten können gelöscht werden, soweit dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Sie sind zu löschen, wenn ihre Speicherung unzulässig war.

(4) Personenbezogene Daten sind am Ende des fünften Jahres nach ihrer Einspeicherung zu sperren, wenn der Betroffene es verlangt.

Die Vorschriften über das Verfahren und die Rechtsfolgen der Sperrung in § 12 Abs. 3 Satz 2 gelten entsprechend.

§ 28

**Verarbeitung personenbezogener Daten
zum Zwecke der Weitergabe
in anonymisierter Form**

(1) Die in § 23 Abs. 1 Nr. 2 genannten Personen, Gesellschaften und anderen Personenvereinigungen sind verpflichtet, die gespeicherten personenbezogenen Daten zu anonymisieren, wenn ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, spätestens am Ende des fünften Jahres nach ihrer Einspeicherung. Die Merkmale, mit deren Hilfe anonymisierte Daten derart verändert werden können, daß sie sich auf eine bestimmte Person beziehen oder eine solche erkennen lassen, sind gesondert zu speichern. Diese Merkmale dürfen mit den anonymisierten Daten nicht mehr zusammengeführt werden, es sei denn, daß die dadurch ermöglichte Nutzung der gesperrten Daten noch für die Erfüllung des Zweckes der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Bei automatischer Datenverarbeitung sind Vorkehrungen zu treffen, daß die Daten nur in dem zulässigen Umfang und in der zulässigen Form weitergegeben und nicht durch Unbefugte abgerufen werden können; die Durchführung der in Absatz 1 vorgesehenen Maßnahmen ist durch entsprechende Vorkehrungen sicherzustellen.

§ 29

**Verarbeitung personenbezogener Daten
im Auftrag Dritter**

(1) Den in § 23 Abs. 1 Nr. 3 genannten Personen, Gesellschaften und anderen Personenvereinigungen sind Weitergabe, Veränderung und Löschung personenbezogener Daten nur mit Zustimmung der Personen oder Stellen gestattet, in deren Auftrag die Daten in Dateien gespeichert und sonst verarbeitet werden.

(2) Bei automatischer Datenverarbeitung sind Vorkehrungen zu treffen, daß die Daten nur in dem zulässigen Umfang weitergegeben, verändert und gelöscht und nicht durch Unbefugte abgerufen werden können.

§ 30

Meldepflichten

(1) Die in § 23 Abs. 1 genannten Personen, Gesellschaften und anderen Personenvereinigungen sowie ihre Zweigniederlassungen und unselbständigen Zweigstellen haben die Aufnahme ihrer Tätigkeit bei der zuständigen Aufsichtsbehörde binnen eines Monats anzumelden.

(2) Bei der Anmeldung sind folgende Angaben zu dem bei der Aufsichtsbehörde geführten Register über die in § 23 Abs. 1 genannten Stellen mitzuteilen:

1. Name oder Firma,
2. Firmeninhaber oder mit der Leitung beauftragte Personen,
3. Anschrift,
4. Zweck des Unternehmens und der Datenverarbeitung,
5. Art der eingesetzten automatischen Datenverarbeitungsanlagen,
6. Art der gespeicherten personenbezogenen Daten.

(3) Absatz 1 gilt für die Beendigung der Tätigkeit sowie für die Änderung der nach Absatz 2 mitgeteilten Angaben entsprechend.

§ 31

Aufsichtsbehörde

(1) Die nach Landesrecht zuständige Aufsichtsbehörde überwacht die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz im Anwendungsbereich dieses Abschnittes. Sie führt das Register über die in § 23 Abs. 1 genannten Personen, Gesellschaften und anderen Personenvereinigungen; das Register kann von jedem, der ein berechtigtes Interesse darlegt, eingesehen werden.

(2) Die Inhaber der nach § 30 Abs. 1 anmeldepflichtigen Stellen und die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozeßordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

(3) Die von der Aufsichtsbehörde mit der Überwachung des Unternehmens beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenden Aufgaben erforderlich ist, Grundstücke und Geschäftsräume des Unternehmens zu betreten, dort Prüfungen und Besichtigungen vorzunehmen und in die geschäftlichen Unterlagen, namentlich in die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme Einsicht zu nehmen. Der Auskunftspflichtige hat diese Maßnahmen zu dulden. Das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) wird insoweit eingeschränkt.

(4) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnittes unterliegenden Gewerbebetriebe bleibt unberührt.

FÜNFTER ABSCHNITT

Straf- und Bußgeldvorschriften

§ 32

Straftaten

(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten

1. weitergibt oder verändert oder
2. abrufen oder sich aus in Behältnissen verschlossenen Dateien verschafft,

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

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

(3) Die Tat wird nur auf Antrag verfolgt.

§ 33

Verletzung der Geheimhaltungspflicht

(1) Wer ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm in seiner Eigenschaft als Angehöriger oder Beauftragter der in § 31 bezeichneten Aufsichtsbehörde bekanntgeworden ist, unbefugt offenbart, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, einen anderen zu schädigen oder sich oder einen anderen zu bereichern, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Ebenso wird bestraft, wer ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm unter den Voraussetzungen des Absatzes 1 bekanntgeworden ist, unbefugt verwertet.

(3) Die Tat wird nur auf Antrag verfolgt.

§ 34

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 20 Abs. 1 in Verbindung mit § 16 Abs. 1, § 26 Abs. 1 in Verbindung mit § 23 Nr. 1 den Betroffenen nicht benachrichtigt,
2. entgegen § 22 Abs. 1 Satz 1 oder 3 einen Beauftragten für den Datenschutz nicht oder nicht rechtzeitig beruft,
3. entgegen § 24 Abs. 2 Satz 3 in Verbindung mit § 23 Nr. 1 die dort bezeichneten Gründe oder Mittel nicht aufzeichnet,
4. entgegen § 30 Abs. 1 und 3 eine Meldung nicht oder nicht rechtzeitig erstattet oder entgegen § 30 Abs. 2 oder 3 bei einer solchen Meldung die erforderlichen Angaben nicht, nicht richtig oder nicht vollständig mitteilt,
5. entgegen § 31 Abs. 2 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 31 Abs. 3 Satz 2 den Zutritt zu den Grundstücken oder Geschäftsräumen oder die Vornahme von Prüfungen und Besichtigungen oder die Einsicht in geschäftliche Unterlagen nicht duldet oder
6. einer Rechtsverordnung nach § 4 Abs. 2 zuwiderhandelt, soweit sie für einen bestimmten Tatbestand auf diese Bußgeldvorschrift verweist.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Deutsche Mark geahndet werden.

SECHSTER ABSCHNITT

Übergangs- und Schlußvorschriften

§ 35

Übergangsvorschriften

(1) Die Veröffentlichung über personenbezogene Daten, die beim Inkrafttreten des Gesetzes schon gespeichert waren, nach § 10 hat binnen eines Jahres nach Inkrafttreten des Gesetzes zu erfolgen.

(2) Die in § 22 Abs. 1 und § 30 Abs. 1 genannten Verpflichtungen treten für die Personen, Gesellschaften und anderen Personenvereinigungen, die bei Inkrafttreten des Gesetzes personenbezogene Daten in Dateien speichern und sonst verarbeiten, mit dem Inkrafttreten des Gesetzes ein.

(3) Sind die zur Person des Betroffenen gespeicherten Daten erstmals vor dem Inkrafttreten des Gesetzes weitergegeben worden, so ist der Betroffene über die Speicherung gemäß § 26 Abs. 1 zu benachrichtigen, wenn die Daten erstmals nach dem Inkrafttreten des Gesetzes weitergegeben werden.

§ 36

Anwendung des Verwaltungsverfahrensgesetzes

Für die Ausführung dieses Gesetzes ist das Verwaltungsverfahrensgesetz auch insoweit anzuwenden, als sie den Ländern obliegt.

§ 37

Weitergeltende Datenschutzvorschriften

Soweit dem Datenschutz dienende besondere Rechtsvorschriften des Bundes auf in Dateien gespeicherte personenbezogene Daten anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Zu den vorrangigen Vorschriften gehören namentlich:

1. Vorschriften über die Geheimhaltung von dienstlich oder sonst in Ausübung des Berufs erworbenen Kenntnissen, z. B. § 12 des Gesetzes über die Statistik für Bundeszwecke vom 3. September 1953 (Bundesgesetzbl. I S. 1314), § 22 der Reichsabgabenordnung, § 9 des Gesetzes über das Kreditwesen vom 10. Juli 1961 (Bundesgesetzbl. I S. 881), §§ 5, 6 des Gesetzes über das Postwesen, §§ 10, 11 des Fernmeldeanlagengesetzes;
2. Vorschriften über das Zeugnis- oder Auskunftsverweigerungsrecht aus persönlichen oder berufsbedingten Gründen in Gerichts- und Verwaltungsverfahren, z. B. §§ 52 bis 55 der Strafprozeßordnung §§ 383, 384 der Zivilprozeßordnung, §§ 177, 178 und 179 der Reichsabgabenordnung;
3. Vorschriften über die Beschränkung oder das Verbot der Weitergabe oder Veröffentlichung von Einzelangaben über Personen, z. B. § 7 Abs. 4, §§ 20 und 22 des Arbeitsförderungsgesetzes vom 25. Juni 1969 (Bundesgesetzbl. I S. 582),

§ 72 Abs. 5 des Berufsbildungsgesetzes vom 14. August 1969 (Bundesgesetzbl. I S. 1112), § 49 des Bundeszentralregistergesetzes;

4. Vorschriften über die Beschränkung der Einsicht in Unterlagen durch Dritte, z. B. § 36 des Gesetzes über das Verwaltungsverfahren der Kriegsopferversorgung vom 2. Mai 1955 (Bundesgesetzbl. I S. 202);
5. Vorschriften über die Einsicht des Beamten oder Arbeitnehmers in seine Personalunterlagen, z. B. § 90 des Bundesbeamtengesetzes, § 83 des Betriebsverfassungsgesetzes;
6. Vorschriften über die Auskunftspflicht von Behörden an Bürger über die zu ihrer Person gespeicherten Daten, z. B. § 1325 der Reichsversicherungsordnung, § 104 des Angestelltenversicherungsgesetzes, § 108 h des Reichsknappschaftsgesetzes;
7. Vorschriften über die Weitergabe, Entfernung und Tilgung von in öffentlichen Registern aufgeführten personenbezogenen Daten, z. B. §§ 19, 23, § 27 Abs. 2, §§ 31, 37 Abs. 1, §§ 39 bis 47 und § 58 des Bundeszentralregistergesetzes, § 30 des Straßenverkehrsgesetzes, § 13 a der Straßenverkehrszulassungs-Ordnung.

Die Verpflichtung zur Wahrung der in § 300 des Strafgesetzbuches genannten Berufsgeheimnisse, z. B. des ärztlichen Geheimnisses, bleibt unberührt.

§ 38

Berlin-Klausel

Dieses Gesetz gilt nach Maßgabe des § 13 Abs. 1 des Dritten Überleitungsgesetzes vom 4. Januar 1952 (Bundesgesetzbl. I S. 1) auch im Land Berlin. Rechtsverordnungen, die auf Grund dieses Gesetzes erlassen werden, gelten im Lande Berlin nach § 14 des Dritten Überleitungsgesetzes.

§ 39

Inkrafttreten

Dieses Gesetz, ausgenommen § 4 Abs. 2, § 11 Abs. 4 und § 15, tritt am ersten Tag des auf die Verkündung folgenden zwölften Kalendermonats in Kraft. § 4 Abs. 2, § 11 Abs. 4 und § 15 treten am Tage nach der Verkündung des Gesetzes in Kraft.

Begründung

A. Allgemeiner Teil

1. Ausgangslage und Ziel des Gesetzes

- 1.1 Die Information gewinnt in der Gesellschaft der westlichen Industrienationen zunehmend an Bedeutung. Der Bürger dieser Gesellschaft betrachtet es als selbstverständlich, in kürzester Frist über wichtige Ereignisse in den fernsten Teilen unseres Erdballs unterrichtet zu werden. Richtige und rechtzeitige Informationen können für Wirtschaftsunternehmen und Individuen von entscheidender Bedeutung sein. Die technischen Hilfsmittel für die schnelle und umfassende Bereitstellung dieser Informationen sind vorhanden und werden ständig fortentwickelt.

Das Informationsbedürfnis kennt indes keine Grenzen; es macht daher auch vor der Privatsphäre des Menschen nicht halt. Ob als Staatsbürger, Bank- oder Kaufhauskunde, Versicherungs- oder Arbeitnehmer, in jeder denkbaren Eigenschaft werden Informationen von ihm oder über ihn gewünscht. Der ihm vom Grundgesetz gewährte Freiheitsraum, die unantastbare Sphäre privater Lebensgestaltung drohen enger und enger zu werden.

Wir stehen zwar erst am Anfang dieser Entwicklung, dennoch ist der Gesetzgeber bereits jetzt aufgerufen, sie durch geeignete Maßnahmen so zu steuern, daß schwerwiegende und kaum reparable Schäden nicht erst eintreten und die Privatsphäre des einzelnen angesichts des technischen Fortschritts, den wir alle wünschen, unantastet bleibt.

- 1.2 Diesem Ziel dient der Entwurf. Er soll den Bürger, in welcher Eigenschaft auch immer er davon betroffen wird, gegen die mißbräuchliche Verwendung der Daten schützen, die sich auf seine persönlichen oder sachlichen Verhältnisse beziehen (personenbezogene Daten). Der seit geraumer Zeit allgemein gebräuchliche, den Kern des Sachverhalts nicht ganz präzise treffende Begriff „Datenschutz“ hat also tatsächlich den Schutz des Menschen bei der Datenverarbeitung zum Inhalt, wohingegen der Schutz der Daten selbst mit dem ebenfalls eingebürgerten Begriff „Datensicherung“ umschrieben wird.

Nun läßt sich der Datenschutz nicht dadurch verwirklichen, daß man die Datenverarbeitung, vor allem die elektronische Datenverarbeitung zum Sündenbock abstempelt und nach dem Vorbild der Maschinenstürmer des Frühkapitalismus eine Lösung in der Beschränkung der Datenverarbeitung sucht. Die öffentliche Verwaltung und die Wirtschaft waren ohne die Datenverarbeitung und die mit ihr verbundenen Rationalisierungsmöglichkeiten nicht mehr funktionsfähig.

Es gilt vielmehr, in den Prozeß der Datenverarbeitung solche Sicherungen einzubauen, die dem Bürger die Gewähr bieten, daß die von ihm weitergegebenen Daten grundsätzlich der von ihm damit gegebenen Zweckrichtung entsprechend verwandt werden, und daß er im übrigen durch eine Reihe von Befugnissen in den Stand gesetzt wird, jederzeit die Richtigkeit der über ihn gespeicherten Daten zu prüfen.

Der Entwurf verfolgt ferner das Ziel, dazu beizutragen, daß sich das Datenschutzrecht in Bund und Ländern möglichst einheitlich entwickelt. Einige Bundesländer haben bereits eigene Datenschutzregelungen erlassen, in anderen liegen den gesetzgebenden Körperschaften Entwürfe vor. Nur ein Tätigwerden des Bundesgesetzgebers, das auch von Landesparlamenten und -regierungen gefordert wird, kann gewährleisten, daß sich der Datenschutz in allen Anwendungsbereichen der Datenverarbeitung gleichartig entwickelt. Aus diesen Gründen wurde mit der Vorbereitung des Regierungsentwurfs eines Bundes-Datenschutzgesetzes frühzeitig begonnen (vgl. Antwort der Bundesregierung vom 5. Oktober 1970 auf eine Kleine Anfrage der Abgeordneten Hirsch, Dichgans, Mertes und Genossen – Drucksache VI/1223). Daneben und unabhängig davon entstand in der Interparlamentarischen Arbeitsgemeinschaft der Initiativentwurf eines Datenschutzgesetzes des Bundes, der als Gesetzentwurf der Abgeordneten Hirsch, Dichgans, Kirst und Genossen (Drucksache VI/2885) in den 6. Deutschen Bundestag eingebracht, jedoch nicht mehr behandelt wurde.

2. Derzeitiger Stand des Datenschutzrechts

- 2.1 Bei der gesetzlichen Regelung des Datenschutzes ist zu berücksichtigen, daß die Forderung, die Privatsphäre des Bürgers zu schützen, nicht neu ist und nicht erst seit dem Einsatz von Computern an unsere Rechtsordnung gestellt wird. Es gibt seit langem eine Fülle von Rechtsvorschriften, die diesem Anliegen Rechnung tragen.

Im öffentlichen Bereich garantieren den Schutz des Individuums an erster Stelle die Grundrechte (Artikel 1 Abs. 1, Artikel 2 Abs. 1 Grundgesetz). Dem Bürger wird damit eine Sphäre privater Lebensgestaltung verfassungskräftig vorbehalten, ein letzter unantastbarer Bereich menschlicher Freiheit, der der Einwirkung der gesamten öffentlichen Gewalt entzogen ist (vgl. auch BVerfGE 6, 32; 27, 1). Der im Grundgesetz verankerte Grundsatz der Gesetzmäßigkeit der Verwaltung gebietet, daß alles Handeln der öffentlichen Gewalt, durch das in die Rechtssphäre des einzelnen eingegriffen wird, unmittelbar auf

die Verfassung oder ein Gesetz im formellen Sinn zurückgeführt werden kann. Daneben gibt es in Einzelgesetzen, im Bürgerlichen Gesetzbuch, im Strafgesetzbuch und in speziellen Verwaltungsgesetzen eine Fülle von Schadensersatz- und Strafvorschriften, von Auskunftsverboten und Geheimhaltungsbestimmungen (vgl. hierzu z. B. das Steuer- und das Statistikgeheimnis), die der öffentlichen Hand in bezug auf die Privatsphäre des Bürgers Schranken setzen. Das Bundeszentralregistergesetz vom 18. März 1971 (Bundesgesetzbl. I S. 243) und der Entwurf eines Bundesmeldegesetzes (Bundestags-Drucksache VI/2654), der in der 6. Legislaturperiode nicht mehr abschließend behandelt werden konnte, enthalten ebenfalls solche Schutzbestimmungen.

Gegen Übergriffe durch private Stellen und Personen wird der Bürger durch bürgerlich-rechtliche und strafrechtliche Normen, vor allem durch das von der Rechtsprechung aus den genannten Grundrechten entwickelte allgemeine Persönlichkeitsrecht geschützt. Es setzt sich gleichsam aus Fallgruppen zusammen und kann so den gesamten Schutzbereich nicht lückenlos abdecken; im übrigen hat es im privaten Rechtsverkehr und gegenüber dem Staat gleichermaßen Geltung. Dem Schutz der Privatsphäre im Wirtschaftsleben dienen direkt oder indirekt Bestimmungen über die behördliche Aufsicht von bestimmten Gewerbebetrieben (wie Auskunfteien, Detekteien, Versicherungen, Kreditinstitute) und Schutzvorschriften in speziellen Wirtschaftsgesetzen wie in dem Gesetz gegen Wettbewerbsbeschränkungen oder in dem Gesetz gegen den unlauteren Wettbewerb.

- 2.2 Alle diese Vorschriften und die dazu ergangene Rechtsprechung haben einen wertvollen Beitrag zur allgemeinen Rechtsentwicklung und zur Förderung des Rechtsbewußtseins geleistet und auch eine wichtige Voraussetzung für die Regelung des speziellen Persönlichkeitsschutzes in der Datenverarbeitung geschaffen.

Den gesamten Bereich der jetzt voraussehbaren Datenschutzbedürfnisse wird diese Vielzahl von unter den verschiedensten Voraussetzungen und Zielvorstellungen geschaffenen Vorschriften aber kaum abdecken können. Hierfür bedarf es eines speziellen Datenschutzgesetzes, das die gesamte Problematik umfassend löst.

- 2.3 Das Bedürfnis nach verstärktem Schutz der Privatsphäre im Bereich der rasch fortschreitenden modernen Datenverarbeitung hat bereits Landesgesetzgeber tätig werden lassen. Durch diese Landesgesetze zum Datenschutz bzw. deren Entwürfe wurden wertvolle Vorarbeiten für ein Bundes-Datenschutzgesetz geleistet.

Das Hessische Datenschutzgesetz vom 7. Oktober 1970 (GVBl. Teil I, S. 625) ist das erste deutsche Gesetz, das sich über einschlägige Regelungen in Einzelgesetzen hinaus, generell mit dem Schutz der Privatsphäre gegen Eingriffe bei der Datenverarbeitung beschäftigt. Es ist in seinem Geltungsbereich auf die Anwendung der maschinellen Datenverarbeitung in der öffentlichen Verwaltung des Landes Hessen beschränkt. Es enthält u. a. Bestimmungen über das Datengeheimnis, das von allen dabei Tätigen zu wahren ist, über den Berichtigungsanspruch des Bürgers bei unrichtig gespeicherten Daten sowie über den Datenschutzbeauftragten, der u. a. die Aufgabe hat, die Einhaltung dieses Gesetzes und der übrigen Datenschutzvorschriften zugunsten des Bürgers zu überwachen.

Auf das Hessische Datenschutzgesetz folgte eine Reihe von Entwürfen zu Datenschutzgesetzen weiterer Länder. Es sind dies zur Zeit

- der Initiativentwurf eines Rheinland-Pfälzischen Landesdatenschutzgesetzes vom 7. Oktober 1970 (Landtagsdrucksache VI 2300), am 15. September 1971 als Drucksache 7/283 mit leicht geändertem Inhalt neu eingebracht,
- der Initiativentwurf eines Nordrhein-Westfälischen Landesgesetzes zum Schutz der Privatsphäre gegen mißbräuchliche Datennutzung vom 11. Juni 1971 (Landtagsdrucksache 7/835),
- der Initiativentwurf eines Hamburgischen Landesdatenschutzgesetzes vom 5. Oktober 1971 (Drucksache VII/1460),
- der Initiativentwurf eines Schleswig-Holsteinischen Gesetzes zum Schutz vor mißbräuchlicher Datennutzung vom 12. Februar 1973 (Drucksache 7/484).

Alle Entwürfe beschränken sich in ihrem Anwendungsbereich auf die öffentliche Verwaltung des jeweiligen Landes. Sie gehen mehr oder weniger deutlich von den Grundlinien des Hessischen Datenschutzgesetzes aus und verfolgen im übrigen – auf unterschiedliche Weise – neue Wege, wobei auch zum Teil Ergebnisse aus der Vorbereitungsarbeit zum Initiativentwurf eines Datenschutzgesetzes des Bundes durch die Interparlamentarische Arbeitsgemeinschaft sowie zu diesem Regierungsentwurf vorangegangenen Referentenentwurf ihren Niederschlag fanden.

Es sind noch Regelungen zu erwähnen, die nicht durch Gesetz, sondern verwaltungsintern getroffen wurden. So hat das Land Schleswig-Holstein die Dienstanweisung über den Schutz der Daten und ihre Geheimhaltung in der Datenzentrale Schleswig-Holstein vom 3. Februar 1970 erlassen. In Niedersachsen gilt der Runderlaß der Niedersächsischen Ministerien über die vorläufige Regelung des Datenschutzes in den Rechenzentren des Landes vom 9. November 1970.

In dem Gesetz über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern vom 12. Oktober 1970 und in dem Gesetz über die Datenzentrale Baden-Württemberg vom 17. November 1970 sind Vorschriften über das Datengeheimnis enthalten.

Ein Blick über die Grenzen der Bundesrepublik hinaus zeigt Bemühungen um spezifische Datenschutzgesetze besonders in anglo-amerikanischen Ländern. Aus den Vereinigten Staaten von Amerika sind Gesetze des Bundes und von Bundesstaaten bekannt geworden, die Teilaspekte regeln. In Kanada wie in Großbritannien hatten Versuche, die Datenschutzproblematik umfassend zu lösen, bisher keinen Erfolg; entsprechende Initiativentwürfe konnten die Zustimmung der gesetzgebenden Körperschaften nicht finden.

3. Grundsatzfragen einer bundesgesetzlichen Regelung

3.1 Den unter 2.1 dargestellten gesetzlichen Regelungen zum Schutz des Persönlichkeitsrechts ist gemeinsam, daß sie im allgemeinen grundsätzlich die Zulässigkeit der Datenspeicherung und -weitergabe voraussetzen und in der Regel nur auf den Inhalt der Daten und den Umgang mit ihnen abstellen. Die kasuistische Rechtsprechung zum allgemeinen Persönlichkeitsrecht geht ebenfalls zumeist nur auf das Wie der Informationsverwertung ein und befaßt sich nicht mit der Vorfrage, ob eine bestimmte personenbezogene Information überhaupt gespeichert werden darf.

Eine wirklich durchschlagende Regelung des Datenschutzes als Persönlichkeitsschutz für den gesamten Bereich der Datenverarbeitung erfordert hier einen neuen Ansatz. Angesichts der heute zur Verfügung stehenden Möglichkeiten und der noch bevorstehenden Entwicklungen in der Datenverarbeitung kann an der Frage, ob personenbezogene Daten gespeichert und in die Verarbeitung im weitesten Sinne einbezogen werden dürfen, nicht vorbeigegangen werden. Die bis heute bekannten rechtlichen, organisatorischen und technischen Vorkehrungen können nicht in allen Fällen mit genügender Sicherheit den unserem Rechtsbewußtsein gemäßen Persönlichkeitsschutz gewährleisten. Eine wirksame gesetzliche Regelung des Datenschutzes muß deshalb prinzipiell von der Fragestellung ausgehen, ob und unter welchen Voraussetzungen personenbezogene Daten überhaupt verarbeitet, das heißt in die schutzrelevanten Phasen der Datenverarbeitung, das sind die Speicherung, Veränderung, Weitergabe und Löschung, eingeführt werden dürfen.

3.2 Eine ausdrückliche Kompetenz des Bundes zur umfassenden gesetzlichen Regelung des Datenschutzes enthält das Grundgesetz nicht. Die Re-

gelungskompetenz für ein Bundes-Datenschutzgesetz ergibt sich durch den Rückgriff auf Gesetzgebungszuständigkeiten für verschiedene Bereiche, die für den Datenschutz von Bedeutung sind. Für den Datenschutz im Anwendungsbereich der öffentlichen Verwaltung ist dies die Gesetzgebungskompetenz für das Verwaltungsverfahren (Artikel 70 ff. in Verbindung mit Artikel 84 Abs. 1, 85 Abs. 1 und 86 des Grundgesetzes). Die Datenverarbeitung wird als Arbeits- und Organisationsmittel eingesetzt und ist damit dem Bereich des Verwaltungsverfahrens zuzuordnen. Bundesrechtliche Datenschutzbestimmungen können daher für die Verwaltungsstätigkeit des Bundes sowie für die der Länder, Gemeinden und Gemeindeverbände erlassen werden, soweit diese Bundesrecht ausführen; im Bereich der landeseigenen Ausführung von Bundesgesetzen bedarf es hierzu der Zustimmung des Bundesrates. Für die gesetzliche Regelung des Schutzes der Privatsphäre in nicht-öffentlichen Bereichen beruht die Gesetzgebungskompetenz des Bundes auf der jeweiligen Sachkompetenz, also auf seiner im Grundgesetz festgelegten Zuständigkeit u. a. für die Gesetzgebung auf dem Gebiet des Wirtschafts-, Arbeits-, Zivil-, Straf- und Prozeßrechts.

3.3 Datenschutzrecht ist eine Querschnittsmaterie, die in eine Vielzahl von Rechts- und Fachgebieten mit ganz unterschiedlichen Sachgesetzlichkeiten hineinwirkt. Eine umfassende bundesgesetzliche Datenschutzregelung, die den besonderen Bedürfnissen in allen einschlägigen Bereichen in vollem Umfang und abschließend gerecht werden wollte, müßte außerordentlich umfangreich, unübersichtlich und perfektionistisch ausfallen. Damit wäre niemandem gedient. Ein entsprechendes Bundesgesetz kann deshalb nur subsidiär gelten; es soll besondere Rechtsvorschriften des Bundes mit Datenschutzcharakter unberührt lassen. Der Entwurf enthält deshalb Bestimmungen, die für spezielle Datenschutzvorschriften in Fachgesetzen gemäß den besonderen Bedürfnissen der jeweiligen Materie Raum lassen.

3.4 Die gegebene – und möglicherweise noch größer werdende – Vielfalt datenschutzrechtlicher Vorschriften der Länder berührt den Bund unmittelbar, da diese unterschiedlichen Länderregelungen auch Geltung haben, soweit Landes- und Kommunalverwaltungen Bundesrecht ausführen. Ein insoweit in Bund und Ländern einheitliches Datenschutzrecht ist im Interesse des Bundes und der Länder wie auch des Staatsbürgers geboten. Durch ein Bundes-Datenschutzgesetz, das für den öffentlichen Bereich unter Ausschöpfung der dem Bund zustehenden Gesetzgebungskompetenz erlassen wird, werden abweichende oder inhaltsgleiche Bestimmungen der Landesgesetze außer Kraft gesetzt.

Soweit Landes- oder Gemeindebehörden Landesrecht ausführen, wird das Bundesgesetz keine Geltung haben. Im Interesse der Rechtseinheit wird sich eine Übernahme der Bundesvorschriften durch die Länder auch für diesen Bereich empfehlen. In der Begründung zum Hessischen Datenschutzgesetz ist z. B. eine Bereitschaft in dieser Richtung zu erkennen.

- 3.5 In nicht-öffentlichen Bereichen, namentlich in der Wirtschaft (z. B. in Auskunfteien, Banken und Versicherungen) bestehen umfangreiche Sammlungen personenbezogener Daten, in denen über zahlreiche Bürger weit in deren Privatsphäre hineinreichende Angaben gespeichert sind. Diese Sammlungen sind gesetzlichen Regelungen bisher weithin entzogen. Während sich der Bürger gegenüber der öffentlichen Verwaltung auf Verfassungsnormen, insbesondere auf Grundrechte sowie auf gesetzliche Schutzbestimmungen berufen kann, befindet er sich gegenüber den Unternehmen der Wirtschaft, die Informationen über ihn sammeln, in einer vergleichsweise ungünstigeren Lage. Der Entwurf bezieht daher neben dem öffentlichen Bereich auch die im privaten Bereich bestehenden Sammlungen personenbezogener Daten ein. Der Datenschutz wird in beiden Bereichen unter Berücksichtigung der jeweiligen Besonderheiten gleichwertig geregelt.

Verbände der unter das Gesetz fallenden Unternehmen, vor allem soweit sie personenbezogene Daten in großen Mengen speichern, haben die Notwendigkeit der Einbeziehung des privaten Bereichs bestritten und zur Begründung vorgebracht, bisher seien Verletzungen der Privatsphäre nicht bekanntgeworden; es gebe in der Wirtschaft wegen des dort herrschenden Wettbewerbs keine Informationsverbundsysteme, wie sie etwa in der öffentlichen Verwaltung geplant seien, und es werde dazu auch nicht kommen. Diese Argumente vermögen nicht zu überzeugen. Wenn hier bisher Verletzungen der Privatsphäre nur selten (etwa durch höchstrichterliche Entscheidungen) allgemein bekannt wurden, dann kann daraus nicht geschlossen werden, daß sie nicht vorgekommen sind; vielmehr wird angenommen werden müssen, daß sie den Betroffenen, da sie ein allgemeines Einsichtsrecht in die sie betreffenden Datensammlungen nicht haben, überhaupt nicht bekanntgeworden sind. Datenaustauschsysteme zwischen branchengleichen, aber auch anderen Unternehmen, sei es auf direktem Wege oder über gemeinsame Datensammelstellen (z. B. bei Dachverbänden), gibt es in erheblichem Umfang; sie beziehen sich auch auf personenbezogene Daten. Dies wurde bei dem im November 1972 vom Bundesministerium des Innern veranstalteten Hearing zum Referentenentwurf eines Bundes-Datenschutzgesetzes besonders deutlich. Mit zunehmender

Erschließung der Möglichkeiten der Datenfernverarbeitung werden diese Datenaustauschsysteme zu automatisierten Informationssystemen ausgebaut. Wenn nicht jetzt Vorsorge getroffen wird, daß dem Schutz der Privatsphäre des Bürgers der ihm zukommende Stellenwert eingeräumt wird, dann wird dies in einem späteren Stadium angesichts der hohen hierfür erforderlichen Investitionen kaum oder nur mit erheblichem Mehraufwand möglich sein.

- 3.6 Das Hessische Datenschutzgesetz und der Rheinland-Pfälzische Gesetzentwurf sind in ihrem Geltungsbereich auf die Anwendung der elektronischen bzw. maschinellen Datenverarbeitung begrenzt. Für diese Beschränkung sprechen mancherlei Erwägungen. Die in der elektronischen Datenverarbeitung liegenden technischen Möglichkeiten des schnellen Transports und der mannigfachen Verknüpfung von Daten lassen hier Gefährdungen der Privatsphäre in der Tat offenkundiger erscheinen, als dies bei der herkömmlichen Datenverarbeitung der Fall ist.

Bei näherer Betrachtung erweist sich aber, daß im Hinblick auf den Schutzzweck des Gesetzes beide Formen der Datenverarbeitung einbezogen werden müssen. Das Gesetz ist als umfassende Regelung für den Umgang mit personenbezogenen Daten in allen schutzrelevanten Phasen der Datenverarbeitung konzipiert worden (vgl. Nr. 3.1). Würde nur ein Teil der in Betracht kommenden Daten, nämlich die elektronisch gespeicherten, vom Gesetz erfaßt werden, bliebe der zur Zeit noch überwiegende Teil der personenbezogenen Daten ungeschützt. Bei den Hinweisen auf die spezifischen Gefahren der elektronischen Datenverarbeitung wird auch vielfach überschen, daß dort die technischen Möglichkeiten der Sicherung ungleich vielfältiger sind, als dies bei der herkömmlichen Datenverarbeitung der Fall ist.

Es wird auch von niemandem ernsthaft bestritten, daß der Bürger durch die herkömmliche Form der Datenverarbeitung ebenfalls erheblich in seiner Privatsphäre beeinträchtigt werden kann. Es wäre ihm kaum verständlich zu machen, wenn er in diesen Fällen schutzlos bliebe.

Es muß ferner bedacht werden, daß im Falle einer Beschränkung des Gesetzes auf die elektronische Datenverarbeitung erhebliche Anreize bestünden, es dadurch zu umgehen, daß die personenbezogenen Daten in gewissen Verfahrensteilen ganz oder teilweise nach herkömmlichen Methoden verarbeitet werden. Die Bundesregierung hält daher die Einbeziehung auch der herkömmlichen Datenverarbeitung grundsätzlich für notwendig.

Gewisse Einschränkungen sind allerdings unvermeidbar und aus Gründen der Praktikabilität zwingend geboten. Einmal schützt das Gesetz

nur personenbezogene Daten, die in Dateien gespeichert sind. Damit soll erreicht werden, daß etwa in Notizblöcken, Akten, Büchern und dergl. gespeicherte Daten nicht unter das Gesetz fallen. Der Entwurf erfaßt darüber hinaus nur Dateien, die Daten enthalten, welche zur Weitergabe an Dritte bestimmt sind. Diese Entscheidung folgte aus der Erwägung, daß Gefährdungen der Privatsphäre in der Regel erst mit der Weitergabe der Daten an Dritte einsetzen und daß daher Dateien, deren Daten zum ausschließlich internen Gebrauch bestimmt sind, nicht unter das Gesetz zu fallen brauchen.

- 3.7 Das Gesetz hat das Ziel, die Privatsphäre des Bürgers im Bereich der Datenverarbeitung zu schützen, ohne jedoch diesen Begriff zu erwähnen oder den Versuch einer Umschreibung oder Definition zu unternehmen (vgl. hierzu die Begründung zu § 1). Die Privatsphäre des Bürgers ist kein allgemeingültig abgrenzbarer Bereich; jeder Mensch zieht ihn je nach seinen konkreten Lebensumständen und der Art seiner Berührungspunkte mit Mitmenschen weiter oder enger.

Dem Gesetzgeber ist es von der Natur der Sache her verwehrt, hier Grenzen zu ziehen. Er muß daher grundsätzlich allen personenbezogenen Daten, soweit sie nicht unmittelbar aus allgemein zugänglichen Quellen entnommen sind, den Schutz dieses Gesetzes angedeihen lassen. Nur dadurch kann ein wirksamer Datenschutz erreicht werden, der insbesondere das unbefugte Zusammensetzen von Einzeldaten zu umfassenden Persönlichkeitsbildern verhindert. Dies geschieht dadurch, daß innerhalb des durch den Anwendungsbereich gezogenen Rahmens personenbezogene Daten nur unter bestimmten Voraussetzungen gespeichert, weitergegeben, verändert und gelöscht werden dürfen. Die Voraussetzungen sind im öffentlichen und privaten Bereich je nach dem Zweck der Verarbeitung unterschiedlich. In keinem Fall dürfen schutzwürdige Belange des Betroffenen beeinträchtigt werden.

- 3.8 Das Gesetz soll auch eine angemessene Kontrolle und Überwachung seiner Datenschutzregelungen vorsehen. Hierfür bieten sich zahlreiche Lösungsmöglichkeiten an. Es könnte nach dem Vorbild des Hessischen Datenschutzgesetzes ein Datenschutzbeauftragter vorgesehen werden. Denkbar wäre auch, einen unabhängigen Ausschuß damit zu betrauen. Als weitere Möglichkeiten wurden eine zentrale Kontrollbehörde oder/und die Einrichtung einer besonderen Gerichtsbarkeit für den Datenschutz vorgeschlagen.

Die Bundesregierung ist der Überzeugung, daß eine einheitliche Fremdkontrolle für den Anwendungsbereich dieses umfassenden Bundes-

gesetzes nur dann effektiv sein würde, wenn sie aus einer weitverzweigten Behördenorganisation bestünde. Dafür sieht die Bundesregierung jedoch keine Notwendigkeit. In der Bundesrepublik wird die Durchführung und Einhaltung der Gesetze bereits in vielfältiger Weise überwacht. Für die öffentliche Verwaltung gilt der Grundsatz der Rechtmäßigkeit allen Handelns, sie untersteht der Kontrolle der Parlamente und ihrer Einrichtungen sowie der unabhängigen Rechnungshöfe. Ihr hierarchischer Aufbau mit parlamentarisch verantwortlichen Ministern an der Spitze enthält zahlreiche Kontrollinstanzen. Die Gerichte gewähren jedem Bürger einen lückenlosen Rechtsschutz. Darüber hinaus hat er das Recht, sich unmittelbar an das Parlament zu wenden.

Angeht dieses gut ausgebauten Kontrollsystems hält es die Bundesregierung im Bereich des Datenschutzes für ausreichend, wenn auf der Grundlage des Prinzips der Selbstverantwortlichkeit ein System abgestufter Selbstkontrolle eingeführt wird. Die öffentliche Verwaltung hat demnach durch geeignete Maßnahmen, die schwerpunktmäßig vorgeschrieben werden, die Durchführung des Gesetzes sicherzustellen. Im nicht-öffentlichen Bereich wird nach der Art der Datenverarbeitung unterschieden und entweder die Bestellung eines der Unternehmensleitung unmittelbar verantwortlichen Beauftragten für den Datenschutz vorgeschrieben oder behördliche Kontrollen vorgesehen.

Ergänzt werden diese Kontrolleinrichtungen dadurch, daß jedermann grundsätzlich das Recht hat, Auskunft über die zu seiner Person gespeicherten Daten zu verlangen. Die Straf- und Bußgeldbestimmungen schließlich tragen das Ihre dazu bei, daß die Vorschriften des Gesetzes von allen Beteiligten eingehalten werden.

- 3.9 In der bisherigen Diskussion traten verschiedentlich Interessengegensätze zutage, unter anderem auch unter dem Gesichtspunkt, ob sich der Teilnehmer in der Rolle des Betroffenen oder des die Daten Speichernden sah. Hierauf wurde in der Antwort der Bundesregierung vom 7. September 1972 auf die Kleine Anfrage der Fraktionen der SPD, FDP (Drucksache VI/3826) schon hingewiesen. Die Bundesregierung hat sich bemüht, einen ausgewogenen Gesetzentwurf vorzulegen, der den Datenschutz gewährleistet, ohne jedoch das legitime Interesse an einer möglichst rationellen Speicherung der notwendigen Informationen zu beeinträchtigen. Daß zu einer Reihe von grundsätzlichen Fragen gleichwohl Meinungen und Forderungen geltend gemacht wurden, die von den im Regierungsentwurf vorgeschlagenen Lösungen abweichen, kann angesichts der Komplexität der Datenschutzmaterie nicht überraschen. Die wesentlichen kontrovers gebliebenen Fragen sind folgende:

- 3.9.1 Der Entwurf trifft Regelungen für öffentliche und private Bereiche und sieht von einer Beschränkung seines Anwendungsbereichs auf die Verwaltung ab. Die Überlegungen sind unter Nr. 3.5 näher dargestellt.
- 3.9.2 Der Anwendungsbereich des Entwurfs wird nicht auf die elektronische Datenverarbeitung beschränkt; es werden auch konventionelle Methoden der Datenverarbeitung einbezogen. Näheres wird dazu unter Nr. 3.6 ausgeführt.
- 3.9.3 Von einer umfassenden, einheitlichen Fremdkontrolle der Durchführung des Datenschutzes wird insbesondere aus Gründen der Praktikabilität abgesehen und das Prinzip der Selbstverantwortlichkeit und einer abgestuften Selbstkontrolle soweit wie möglich verfolgt. Auf Einzelheiten wird unter Nr. 3.8 näher eingegangen.
- 3.9.4 Der Entwurf schützt nur Daten über natürliche Personen, obwohl nicht zu verkennen ist, daß auch juristische Personen (z. B. Kapitalgesellschaften oder eingetragene Vereine) oder nichtrechtsfähige Personengruppen (z. B. offene Handelsgesellschaften oder auch Wohngemeinschaften) über einen Innenbereich verfügen, der gegenüber dem Informationsbedürfnis Dritter Schutz verdient. Weil aber dieser Bereich gesetzgeberisch kaum faßbar ist und die Praktikabilität des Entwurfs beeinträchtigen könnte, hat die Bundesregierung darauf verzichtet, diese Personengruppen als Schutzobjekt mit aufzunehmen. Soweit davon auch juristische Personen des Handelsrechts betroffen sind, entspricht dies im übrigen deren Wünschen. Es konnte jedoch nicht so weit gegangen werden, wie vorgeschlagen wurde, auch natürliche Personen vom Schutz des Gesetzes auszunehmen soweit sie wettbewerbsfähig am Wirtschaftsleben teilnehmen, schon deshalb nicht, weil eine Abgrenzung zwischen den personenbezogenen Daten, die hierauf Bezug haben, und anderen Daten über ein und dieselbe Person kaum möglich ist und eine solche Regelung deshalb zu Rechtsunsicherheiten führen würde.
- 3.9.5 Ähnliches gilt für die Beschränkung des Anwendungsbereichs des Gesetzes auf personenbezogene Daten, die in Dateien gespeichert und zur Weitergabe an Dritte bestimmt sind. Auch hier war abzuwägen zwischen dem Interesse des Betroffenen an einem umfassenden Schutz seiner Daten, wo und zu welchem Zweck auch immer sie gespeichert sein mögen, und der Notwendigkeit, das Gesetz praktikabel zu gestalten. Ein Verzicht auf diese Beschränkung hätte zur Folge gehabt, daß auch Notizbücher, Akten und kleine nur zum persönlichen Gebrauch bestimmte Handkarteien unter das Gesetz gefallen wären. Dies ist jedoch bisher weder gefordert worden noch wäre es möglich, das Gesetz dann noch wirksam durchzuführen.
- 3.9.6 Es ist weiter erwogen worden, durch generelle Vorschrift das Gesetz für nicht anwendbar zu erklären, wenn dies aus Gründen der öffentlichen Sicherheit oder Ordnung geboten ist. Dies hätte auf die Weise geschehen können, daß die Sicherheitsbehörden aus dem Anwendungsbereich ausgenommen worden wären oder daß im allgemeinen Teil neben die Zulässigkeitsvoraussetzungen der Zustimmung des Betroffenen und der Rechtsvorschrift eine weitere aufgenommen worden wäre, die die Verarbeitung personenbezogener Daten auch in diesen Fällen gestattet. Davon ist jedoch abgesehen worden, weil durch eine so allgemeine Bestimmung der Datenschutz ernsthaft in Frage gestellt worden wäre. Für solche Ausnahmenvorschriften besteht aber auch kein Bedürfnis. Die Bundesregierung hat sich bemüht, das Gesetz in seinen Einzelbestimmungen so zu gestalten, daß Sicherheit und Ordnung, namentlich auch die Verbrechensbekämpfung, durch dieses Gesetz nicht beeinträchtigt werden.
- 3.9.7 Einige einschlägige Gesetzentwürfe enthalten Bestimmungen, durch die die speichernden Stellen zur Führung eines Protokolls verpflichtet werden, in dem die weitergegebenen Daten, deren Empfänger und der Zeitpunkt der Weitergabe festgehalten werden. Auch in der Literatur wird die Protokollierung vielfach als unabdingbare Voraussetzung für einen wirksamen Datenschutz gefordert.
- Die Protokollierung dient primär dem Zweck, es dem Betroffenen zu ermöglichen, die Stellen, an die Daten über ihn weitergegeben worden sind, zu ermitteln und im Wege der Auskunftseinholung prüfen zu können, ob diese Daten dort richtig und auch zulässigerweise gespeichert worden sind. Dies ist indes nach dem Entwurf auch ohne das Protokollierungsverfahren möglich. Nach § 10 sind die im zweiten Abschnitt genannten speichernden Stellen verpflichtet, die Öffentlichkeit in geeigneter Weise über die Art der von ihnen gespeicherten personenbezogenen Daten sowie die betroffenen Personengruppen zu unterrichten. Der Bürger kann daraus ersehen, wo Daten über ihn gespeichert sein könnten, und sodann gezielt Auskunft verlangen. Gibt eine Behörde personenbezogene Daten an eine nicht-öffentliche Stelle weiter, die sie ihrerseits in einer Datei speichert, ist diese je nach dem Zweck der von ihr betriebenen Datenverarbeitung grundsätzlich verpflichtet, den Betroffenen nach §§ 20 oder 26 von der Speicherung zu unterrichten. Werden personenbezogene Daten nach den Bestimmungen des dritten oder vierten Abschnitts weitergegeben (§§ 18, 24) und von dem Empfänger in einer Datei gespeichert, ist der Betroffene ebenfalls nach §§ 20 oder 26 zu benachrichtigen.

Der durch diese Benachrichtigungspflicht nach §§ 20 oder 26 entstehende Mehraufwand kann überdies erheblich reduziert werden, wenn der Betroffene möglichst frühzeitig, etwa während der Vertragsverhandlungen, unterrichtet wird, an welche Stellen die Daten weitergegeben werden sollen. In solchen Fällen bedarf es der Benachrichtigung nicht mehr.

Darüber hinaus dient die Protokollierung aber auch Kontroll- und Präventivzwecken, z. B. dazu, den unbefugten Zugriff auf personenbezogene Daten festzustellen. Auf diese Art der Protokollierung kann nicht verzichtet werden; denn personenbezogene Daten, die in automatisierten Datenverarbeitungsanlagen auf Abruf bereitstehen und bei Bedarf selbsttätig – ohne vorherige menschliche Kontrolle – dem Empfänger zufließen, sind dem unbefugten Zugriff in besonderem Maße ausgesetzt. Für diese Fälle wird deshalb die Führung eines Protokolls vorgeschrieben, damit die nachträgliche Kontrolle voll gewährleistet bleibt.

4. Grundzüge des Gesetzes

4.1 Die Regelungen des Gesetzes sind vor dem Hintergrund der noch nicht abgeschlossenen Entwicklung der Datenverarbeitung und der damit zusammenhängenden Gebiete der Technik und Organisation und des Rechts zu sehen. Angesichts der in Wissenschaft und Praxis noch offenen Fragen über die auf Dauer optimale organisatorische, technische und rechtliche Ausgestaltung des Datenschutzes war dem Gesetz eine Konzeption zugrunde zu legen, die nach heutigem Stand der Erkenntnis einen wirkungsvollen Datenschutz in verfassungsgemäßer Weise gewährleistet, die Alltagspraxis in Verwaltung und Wirtschaft nicht unnötig behindert, den technischen Fortschritt nicht hemmt und das Vertrauen des Bürgers zum Staat im Zeitalter des Computers bewahrt.

4.2 Die wesentlichen Grundzüge des Gesetzes sind folgende:

4.2.1 Das Gesetz gibt dem Datenschutz dienenden besonderen Rechtsvorschriften des Bundes, soweit sie auf in Dateien gespeicherte personenbezogene Daten anzuwenden sind, Vorrang (§ 37). Damit wird für spezielle Datenschutzregelungen in Fachgesetzen gemäß den besonderen Bedürfnissen der jeweiligen Materie Raum gelassen und eine perfektionistische Lösung in diesem Gesetz vermieden.

4.2.2 Gegenstand des Datenschutzes sind personenbezogene Daten, die bei bestimmten öffentlichen oder privaten Stellen in Dateien gespeichert oder sonst verarbeitet werden (§ 2). Per-

sonenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer natürlichen Person (§ 3 Abs. 1).

4.2.3 Geregelt wird der Umgang mit personenbezogenen Daten in allen schutzrelevanten Phasen der Datenverarbeitung, das sind die Speicherung, Weitergabe, Veränderung und Löschung der Daten. Davon werden vor allem die kritischen Bereiche des Dateneingangs und -ausgangs betroffen und so der unkontrollierte Daten- und Informationskreislauf unterbrochen

4.2.4 Die Regelung erstreckt sich auf die elektronische und auf die herkömmliche Datenverarbeitung (§ 3 Abs. 2). Die herkömmlichen Methoden werden in der Praxis auf absehbare Zeit noch erhebliche Bedeutung haben; sie können ohne Schaden nicht ausgeklammert werden. Eine Beschränkung auf die EDV würde zu einer Ungleichbehandlung führen und Gesetzesumgehungen ermöglichen oder sogar herausfordern.

4.2.5 Ein wirkungsvolles Bundesgesetz muß den Datenschutz in der öffentlichen Verwaltung und in privaten Bereichen unter Berücksichtigung der jeweiligen Besonderheiten gleichwertig regeln. Auch dadurch werden Ungleichbehandlungen und Gesetzesumgehungen vermieden.

4.2.6 Das Gesetz enthält folgende Anwendungsgebiete:

- a) Im Bereich der öffentlichen Verwaltung wird die Verarbeitung personenbezogener Daten durch Behörden und sonstige Stellen
- des Bundes,
 - der Länder, Gemeinden und Gemeindeverbände, soweit sie Bundesrecht ausführen,

erfaßt (zweiter Abschnitt § 5 Abs. 1). Es war außerdem notwendig, auch die Fälle zu regeln, in denen Behörden und sonstige öffentliche Stellen personenbezogene Daten durch andere Stellen speichern und verarbeiten lassen oder selbst im Auftrag anderer datenverarbeitend tätig werden (§ 5 Abs. 3). Nach § 5 Abs. 5 fallen auch die sog. beliebigen Unternehmer (z. B. Technische Überwachungsvereine) unter die Bestimmungen des zweiten Abschnitts.

- b) Im nicht-öffentlichen Bereich erfaßt das Gesetz einmal die interne Verarbeitung von personenbezogenen Daten durch Personen Unternehmen und sonstige Stellen (z. B. bei

- Banken, Versicherungen, Handelsfirmen, Verbänden) – dritter Abschnitt, § 16 –, darüber hinaus
- c) die geschäftsmäßige Datenverarbeitung nicht-öffentlicher Stellen für Dritte. Darunter fällt
- die Speicherung personenbezogener Daten zum Zwecke ihrer Weitergabe sowie die Weitergabe (z. B. durch Auskunfteien) – vierter Abschnitt, § 23 Abs. 1 Nr. 1,
 - die Weitergabe in anonymisierter Form (z. B. durch Markt- und Meinungsforschungsinstitute) – vierter Abschnitt, § 23 Abs. 1 Nr. 2,
 - die Speicherung und sonstige Verarbeitung im fremden Auftrag (z. B. durch Dienstleistungs-Rechenzentren) – vierter Abschnitt, § 23 Abs. 1 Nr. 3.
- 4.2.7 Die Regelung der Zulässigkeit jeder Verarbeitung von personenbezogenen Daten stellt in jeder Verarbeitungsphase, differenziert nach den Anwendungsbereichen, auf den jeweiligen Sachzweck ab, der mit Hilfe der Datenverarbeitung erfüllt werden soll.
- 4.2.8 In allen Bereichen wird dem Bürger ein grundsätzliches Recht gewährt auf
- Auskunft über die zu seiner Person gespeicherten Daten,
 - Berichtigung, wenn die ihn betreffenden Daten unrichtig gespeichert sind,
 - Sperrung, wenn der zulässige Speicherungszweck weggefallen ist,
 - Löschung, wenn die Speicherung unzulässig war.
- Die Rechte sind in den Anwendungsbereichen (4.2.6) differenziert geregelt (zweiter Abschnitt: §§ 11, 12; dritter Abschnitt §§ 20, 21; vierter Abschnitt: §§ 26, 27).
- 4.2.9 Das Gesetz regelt die Kontrolle der Durchführung des Datenschutzes in allen Anwendungsbereichen. Dabei wird das Prinzip der Selbstverantwortlichkeit und Selbstkontrolle weitgehend verwirklicht. Grundsätzlich treffen die Stellen, die personenbezogene Daten verarbeiten, die erforderlichen Maßnahmen selbst. In Verbindung mit weiteren Vorkehrungen (Auskunftsrecht des Betroffenen, Straf- und Bußgeldvorschriften) wird damit eine wirksame Kontrolle gewährleistet. Von der Einrichtung einer zentralen Kontrollinstitution wird abgesehen.
- 4.3 Der Gesetzentwurf ist in seinem Aufbau wie folgt gegliedert:
- Der erste Abschnitt enthält allgemeine Vorschriften, die für die in den zweiten bis vierten Abschnitten geregelten Anwendungsbereiche gemeinsam gelten. Dazu gehören die Regelung des Anwendungsbereichs des Gesetzes sowie von Inhalt und Gegenstand des Datenschutzes und von Maßnahmen der Datensicherung (§§ 1 bis 4).
- Im zweiten Abschnitt ist die Datenverarbeitung durch öffentliche Stellen geregelt, und zwar der Anwendungsbereich (§ 5), die relevanten Phasen der Datenverarbeitung (§§ 6 bis 9), die Bekanntmachung der gespeicherten Daten, Auskunftserteilung sowie Berichtigung, Löschung und Sperrung von Daten (§§ 10 bis 12) und die Durchführung des Datenschutzes (§§ 14, 15). Die Verarbeitung personenbezogener Daten im Auftrag anderer Behörden und sonstiger öffentlicher Stellen wird in § 13 geregelt.
- Im dritten Abschnitt ist die Regelung der Datenverarbeitung im nicht-öffentlichen Bereich für interne Zwecke vorgesehen. Der Aufbau folgt hier – wie auch im vierten Abschnitt – der gleichen Systematik wie im zweiten Abschnitt: Anwendungsbereich (§ 16), regelungsbedürftige Verarbeitungsphasen (§§ 17 bis 19), Anspruch auf Auskunft, Berichtigung, Löschung und Sperrung (§§ 20, 21) und Durchführung des Datenschutzes (§ 22).
- Der vierte Abschnitt enthält Datenschutzbestimmungen für die privaten Unternehmen, die personenbezogene Daten geschäftsmäßig für Dritte verarbeiten. Es werden geregelt der Anwendungsbereich (§ 23), die relevanten Verarbeitungsphasen (§§ 24, 25), Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsanspruch (§§ 26, 27), die besonderen Anwendungsfälle der Beschaffung von personenbezogenen Daten zum Zwecke der Weitergabe in anonymisierter Form und der Datenverarbeitung im Auftrag Dritter (§§ 28, 29), sowie Überwachung des Datenschutzes (§§ 30, 31).
- Es folgen im fünften Abschnitt Straf- und Bußgeldbestimmungen (§§ 32 bis 34) sowie im sechsten Abschnitt Übergangs- und Schlußvorschriften (§§ 35 bis 39).
5. Kosten
- 5.1 Durch die Ausführung dieses Gesetzes werden der Bund, die Länder und Gemeinden sowie die betroffenen nicht-öffentlichen Stellen mit zusätzlichen Kosten in unterschiedlicher Höhe belastet.
- Generell ist zur Höhe der voraussichtlich entstehenden Kosten festzustellen, daß ein erheblicher Teil der von diesem Gesetz vorgesehenen

Schutzmaßnahmen aus anderen Gründen, insbesondere nach den Grundsätzen ordnungsgemäßer Datenverarbeitung einschließlich der Datensicherung, ohnehin erbracht werden muß. Der Verhältnismäßigkeitsgrundsatz des § 4 verhindert darüber hinaus einen übermäßigen Kostenaufwand aus Gründen des Datenschutzes. Die bei der Auskunftserteilung entstehenden Kosten werden durch Gebühren bzw. privatrechtliche Entgelte abgedeckt.

- 5.2 Die vom Bund zu tragenden zusätzlichen Kosten resultieren im wesentlichen aus der Verpflichtung zur Veröffentlichung nach § 10, aus Maßnahmen zur Sicherstellung der Ausführung des Gesetzes nach § 14, und aus zusätzlichen Datensicherungsmaßnahmen. Weiter können sich näher noch nicht feststellbare Kosten für den Bund daraus ergeben, daß Vorkehrungen getroffen werden müssen, um Auskünfte zu erteilen. Nach einer überschlägigen Schätzung wird die Kostenlast für den Bund insgesamt durchschnittlich etwa 1 Mio DM jährlich ausmachen. Die Kosten können im Rahmen des nach der derzeitigen Finanzplanung geltenden Plafonds aufgefangen werden.
- 5.3 Soweit die Länder, Gemeinden und Gemeindeverbände bei der Ausführung von Bundesrecht personenbezogene Daten verarbeiten, haben sie die aus der Anwendung dieses Gesetzes entstehenden Kosten nach dem Grundsatz des Artikel 104 a Abs. 1 und Abs. 5 GG zu tragen. Dabei ist zu berücksichtigen, daß die Verarbeitung personenbezogener Daten in Ausführung von Landesrecht von den Landesdatenschutzgesetzen geregelt wird. Die insoweit entstehenden Kosten können im allgemeinen nur schwer von den durch dieses Gesetz zusätzlich verursachten Kosten getrennt werden. Der bei den Aufsichtsbehörden nach § 31 zusätzlich anfallende Personal- und Sachaufwand ist zur Zeit nicht bezifferbar.
- 5.4 Die von dem Gesetz betroffenen nicht-öffentlichen Stellen haben die ihnen bei der Verarbeitung personenbezogener Daten durch das Gesetz entstehenden Mehrkosten selbst zu tragen. Für die unter den dritten Abschnitt fallenden Stellen wirkt sich vor allem die in § 22 vorgesehene Bestellung eines Beauftragten für den Datenschutz kostenwirksam aus. Dabei ist allerdings zu berücksichtigen, daß – zumindest in größeren Unternehmen – nach schon vielfach vertretener Ansicht ein Betriebsbeauftragter für Datensicherung ohnehin erforderlich ist, der auch diese im Gesetz vorgesehenen Aufgaben übernehmen sollte. Diese Kosten können insgesamt zur Zeit auch nicht annähernd angegeben werden. Die nach §§ 20 und 26 vorgesehene Verpflichtung zur Benachrichtigung über die Speicherung von personenbezogenen

Daten verursacht ebenfalls – in der Regel nicht erhebliche – Kosten, die indes ziffernmäßig nicht fixierbar sind. Die in gewerblichen Unternehmen anfallenden Kosten gehen im allgemeinen als betriebliche Aufwendungen in die Gewinn- und Verlustrechnung ein.

- 5.5 Auf das allgemeine Verbraucherpreisniveau wird sich das Gesetz nicht auswirken. Auswirkungen auf Einzelpreise sind nur vereinzelt zu erwarten, da die durch das Gesetz verursachten Mehrkosten im Verhältnis zum Gesamtumsatz der betroffenen Unternehmen nur geringfügig sein dürften.

B. Zu den einzelnen Vorschriften

Zum ersten Abschnitt – Allgemeine Vorschriften

Zu § 1 – Zweck des Gesetzes

§ 1 nennt das von diesem Gesetz primär geschützte Rechtsgut, die schutzwürdigen persönlichen Belange. Damit soll der Bereich umschrieben werden, der in der einschlägigen Literatur und Rechtsprechung mit den Begriffen „Privatsphäre“, „Persönlichkeitsrecht“ oder dergl. versehen wird. Zugleich wird daraus, daß der Schutz der personenbezogenen Daten an erster Stelle genannt wird, deutlich, daß wegen der Relativität der Privatsphäre (vgl. Allgemeiner Teil der Begründung Nr. 3.7) die schutzwürdigen persönlichen Belange nicht unmittelbar, sondern nur auf dem Umweg über den Schutz der personenbezogenen Daten gewahrt werden können.

Zu § 2 – Gegenstand des Datenschutzes

Absatz 1 faßt den Anwendungsbereich des Gesetzes zusammen; er wird in den in Nr. 1 bis 3 zitierten Bestimmungen näher umschrieben. Zur Frage der Beschränkung auf Dateien, deren Daten zur Weitergabe an Dritte bestimmt sind, wird auf den Allgemeinen Teil der Begründung Nr. 3.6 und 3.9.5 verwiesen.

Die Regelung des Absatzes 2 ist eine Konsequenz aus dem Grundrecht der Informationsfreiheit (Artikel 5 Abs. 1 Satz 1 GG). Die Beschränkung auf personenbezogene Daten, die den allgemein zugänglichen Quellen (z. B. Zeitungen, Adreßbücher, Fernsprechverzeichnisse) unmittelbar entnommen sind, ist allerdings auf Kritik gestoßen. Sie ist indes notwendig, um zu verhindern, daß solchen Quellen entnommene und in verschiedenen Dateien gespeicherte Daten durch Verknüpfung mit anderen zu einem umfassenden Persönlichkeitsdossier zusammengefügt werden können. Die Ausnahmebestimmung des Satzes 2 des Absatzes 2 sieht vor, daß das Gesetz nicht für die Speicherung und Weitergabe von personenbezogenen Daten durch Unternehmen und Hilfsunternehmen der Presse, des Rundfunks und des Films gilt, soweit diese Datenverarbeitung vom

Grundrecht der Pressefreiheit bzw. der Freiheit der Berichterstattung (Artikel 5 Abs. 1 Satz 2 GG) geschützt wird. Die Grenzen der Datenverarbeitung werden insoweit durch die Vorschriften über diese Grundrechte und die dazu ergangene Rechtsprechung gezogen.

Absatz 3 nennt zwei für das ganze Gesetz geltende Zulässigkeitsvoraussetzungen für die Verarbeitung von personenbezogenen Daten, nämlich die Zustimmung des Betroffenen und ermächtigende Rechtsvorschriften. Weitere auf besondere Sachverhalte zugeschnittene Zulässigkeitsvoraussetzungen ergeben sich aus einzelnen Bestimmungen des Gesetzes. An dieser Stelle wird auch festgelegt, daß die Zustimmung grundsätzlich der Schriftform bedarf; der Betroffene muß ausdrücklich auf die Zustimmungserklärung hingewiesen werden, wenn er sie zusammen mit anderen Willenserklärungen, etwa im sog. Kleingedruckten eines Bestell- oder Auftragssscheins oder dergl., abgibt.

Zu § 3 – Begriffsbestimmungen

Die Vorschrift legt fest, wie die wesentlichen Begriffe dieses Gesetzes zu verstehen sind. Mit den Begriffsbestimmungen sind zugleich Entscheidungen über den Anwendungsbereich des Gesetzes getroffen worden. Der in Absatz 1 umschriebene Begriff „personenbezogene Daten“ beschränkt sich auf Daten über natürliche Personen (vgl. dazu den Allgemeinen Teil der Begründung Nr. 3.9.4). Der in Absatz 2 Nr. 1 definierte Begriff „Datenverarbeitung“ umfaßt sowohl die elektronische als auch die herkömmliche Datenverarbeitung (vergl. dazu den Allgemeinen Teil der Begründung Nr. 3.6). Der unter Absatz 2 Nr. 2 aufgeführte Begriff „Speichern“ beschränkt sich auf den Vorgang der Aufbewahrung der Daten auf gewisse Dauer, er umfaßt also nicht den Fall, daß Daten nur zu einem bestimmten Zweck (z. B. Auftragsabwicklung) in den Kernspeicher der EDV-Anlage aufgenommen, verarbeitet und sodann wieder gelöscht werden. Die sonstigen schutzrelevanten Phasen der Datenverarbeitung (Verändern, Weitergeben, Löschen) werden ebenfalls definiert. Mit dem in Absatz 3 definierten Begriff „Datei“ werden nach elektronischen und herkömmlichen Verfahren geführte Datensammlungen erfaßt. Darunter fallen nach bestimmten Merkmalen organisierte bzw. organisierbare und deshalb leicht zugängliche und auswertbare Datensammlungen wie z. B. Sichtlochkarteien, nicht jedoch Akten, Akten-sammlungen oder Bücher.

Zu § 4 – Technische und organisatorische Maßnahmen des Datenschutzes

Es gibt eine Vielzahl von Möglichkeiten, den Datenschutz durch technische und organisatorische Einrichtungen und Verfahren zu verbessern. Das gilt vor allem für die Datenverarbeitung mit Hilfe automatischer Methoden. Es empfiehlt sich jedoch schon deshalb nicht, spezielle Maßnahmen solcher Art im Gesetz im einzelnen vorzuschreiben, da diese Be-

stimmungen bald durch die fortschreitende technische Entwicklung überholt sein würden. Das Gesetz mußte sich mit Bestimmungen über technische und organisatorische Sicherungsmaßnahmen allgemeineren Inhalts begnügen (vgl. z. B. § 7 Abs. 3, § 9 Abs. 2).

§ 4 Abs. 1 bestimmt als Grundsatz, daß jeder, der personenbezogene Daten verarbeitet, die auf Grund des Gesetzes notwendigen Datenschutzmaßnahmen zu treffen hat. Es sind das einmal die nach Maßgabe des Einzelfalls notwendigen Datensicherungsmaßnahmen, die allen gespeicherten Daten zugute kommen; sodann organisatorische und technische Vorkehrungen, durch die die korrekte Durchführung der Bestimmungen dieses Gesetzes gewährleistet wird. Satz 2 stellt sicher, daß der Datenschutz nicht zum Selbstzweck und durch die notwendigen Schutzmaßnahmen der mit der Datenverarbeitung beabsichtigte Rationalisierungseffekt nicht verhindert wird.

§ 4 Abs. 2 ermächtigt die Bundesregierung, durch Rechtsverordnung mit Zustimmung des Bundesrates Grundsätze über die in den einzelnen Anwendungsbereichen zur Regelung der jeweiligen Verarbeitungsphasen erforderlichen technischen und organisatorischen Maßnahmen des Datenschutzes zu erlassen sowie bestimmte Maßnahmen unmittelbar vorzuschreiben; in letzterer Hinsicht kann die Ermächtigung auch auf die Landesregierungen übertragen werden. Für den nicht-öffentlichen Bereich bleibt die Verordnungszuständigkeit beim Bund, damit der Datenschutz dort einheitlich ausgestaltet wird. Für Unternehmen mit Betriebsstätten in mehreren Ländern ist dies von erheblicher Bedeutung.

Zum zweiten Abschnitt – Datenverarbeitung der Behörden und sonstigen öffentlichen Stellen

Zu § 5 – Anwendungsbereich

Nach Absatz 1 gelten die Vorschriften des zweiten Abschnittes für die Verarbeitung personenbezogener Daten durch Behörden und alle sonstigen Stellen des Bundes einschließlich der Bundesgerichte und der Bundesanwaltschaften, und seiner juristischen Personen des öffentlichen Rechts sowie durch Behörden und sonstige Stellen der Länder (einschließlich der Gerichte und Staatsanwaltschaften), Gemeinden, Gemeindeverbände und deren juristischen Personen des öffentlichen Rechts – hier mit Ausnahme der §§ 14 und 15 –, soweit diese Bundesrecht ausführen. Zur Bindung der Länder auf diesem Gebiet an die Vorschriften des Bundes wird auf die Ausführungen im Allgemeinen Teil der Begründung (Nr. 3. 4) Bezug genommen.

Durch Absatz 2 werden an sich unter Absatz 1 fallende öffentliche Stellen aus dem Anwendungsbereich des zweiten Abschnittes – mit Ausnahme der §§ 13 bis 15 – ausgenommen, die am wirtschaftlichen Wettbewerb teilnehmen. Für sie gilt nach § 16 Abs. 1 der dritte Abschnitt.

Absatz 3 dient dem Zweck, den Anwendungsbereich möglichst lückenlos zu gestalten und die Fälle zu erfassen, in denen Behörden und sonstige öffentliche Stellen personenbezogene Daten durch andere Stellen speichern und verarbeiten lassen oder selbst im Auftrag anderer datenverarbeitend tätig werden. Dabei war der Gedanke leitend, daß das ausführende Rechenzentrum Erfüllungsgehilfe ist, während die auftraggebende Behörde Herr über die Daten bleiben soll, die sie zur Erfüllung ihrer Verwaltungsaufgaben benötigt.

Absatz 4 bestimmt eine weitere Ausnahme von Absatz 1. Auf die an sich unter Absatz 1 fallende Datenverarbeitung in Zusammenhang mit dienst- und arbeitsrechtlichen Rechtsverhältnissen finden vom zweiten Abschnitt nur die §§ 13 bis 15 Anwendung. Im übrigen gelten dafür die §§ 17 bis 21 aus dem dritten Abschnitt entsprechend. Der Grund dafür liegt darin, daß die Vorschriften dieses Abschnittes für die Regelung von Dienst- und Arbeitsverhältnissen, auch soweit sie mit der öffentlichen Hand begründet sind, besser geeignet sind; damit wird auch erreicht, daß alle Arbeitsverhältnisse datenschutzrechtlich einheitlich nach denselben Vorschriften behandelt werden. Die Erstreckung auf frühere und künftige Rechtsverhältnisse trägt der Tatsache Rechnung, daß Wehrpflichtige sowohl vor als auch nach ihrer Dienstzeit erfaßt werden müssen.

Der Behördenbegriff in Absatz 5 ist dem Regierungsentwurf eines Verwaltungsverfahrensgesetzes entnommen. Er fußt auf der Rechtsprechung zur Verwaltungsgerichtsordnung und ist nicht im organisationsrechtlichen Sinne zu verstehen. Er schließt auch natürliche und juristische Personen ein, die als sogenannte beliehene Unternehmer öffentlich-rechtliche Verwaltungstätigkeit ausüben.

Zu § 6 – Datenspeicherung

Diese Vorschrift regelt die Datenspeicherung als besonders wichtige schutzrelevante Phase der Datenverarbeitung, denn mit der Speicherung entsteht zugleich die Gefahr der mißbräuchlichen Nutzung. Sie ist daher abgesehen von der Zustimmung des Betroffenen oder auf Grund einer Rechtsvorschrift (§ 2 Abs. 3) nur im Rahmen der rechtmäßigen Aufgabenerfüllung zulässig. Im letzteren Fall hängt die Zulässigkeit von zwei Voraussetzungen ab, nämlich von der Erforderlichkeit ihrer Kenntnis für die Aufgabenerfüllung sowie von der Zuständigkeit der Behörde für die Erfüllung gerade dieser Aufgabe. Damit wird ein unnötiges Eindringen in den Persönlichkeitsbereich verhindert und dem Zusammenströmen aller Informationen über eine Person zu einem geschlossenen Persönlichkeitsbild eine Grenze gesetzt.

Der Rahmen rechtmäßiger Aufgabenerfüllung kann in Einzelfällen auch durch einen privatrechtlichen Vertrag ausgefüllt und abgegrenzt werden, etwa dann, wenn in einem öffentlichen Krankenhaus ein Patient auf Grund eines privatrechtlichen Vertrages behandelt wird.

Wer als „speichernde Stelle“ im Sinne dieses Gesetzes anzusehen ist, ergibt sich aus § 5 Abs. 3 in Verbindung mit § 13 des Entwurfs. Diese Bestimmungen sehen vor, daß eine Behörde auch dann für den Datenschutz verantwortlich bleibt, wenn sie die Datenverarbeitung „außer Haus“ betreibt.

Zu § 7 – Datenaustausch innerhalb der öffentlichen Verwaltung

In Absatz 1 wird der Datenaustausch geregelt. Darunter wird die Weitergabe von personenbezogenen Daten zwischen den unter den zweiten Abschnitt fallenden Behörden und Stellen sowie an andere Behörden und Stellen des öffentlichen Bereichs verstanden. Zu diesen Empfängern zählen auch Stellen von juristischen Personen des öffentlichen Rechts, die nach § 5 nicht zum Anwendungsbereich dieses Abschnittes gehören, also z. B. Behörden der Länder und Gemeinden, auch soweit sie nicht Bundesrecht ausführen.

Personenbezogene Daten, die der Bürger einer Behörde oder sonstigen öffentlichen Stelle anvertraut hat, werden vor einer Preisgabe an Außenstehende in der Regel dadurch geschützt, daß die mit der Bearbeitung dieser Daten betrauten Behördenbediensteten durch Spezialvorschriften in den jeweils auszuführenden Gesetzen (z. B. § 33 dieses Gesetzes) zur Verschwiegenheit verpflichtet sind. Ebenfalls hinlänglich geschützt sind personenbezogene Daten, die einer zur Wahrung des Berufsgeheimnisses verpflichteten Person (z. B. Arzt) anvertraut worden sind. Absatz 1 Satz 1 soll dem Bürger die Gewißheit geben, daß solche Daten auch denn noch besonders geschützt bleiben, wenn sie von der nach einem Berufs- oder besonderen Amtsgeheimnis zur Verschwiegenheit verpflichteten Person unter Beachtung der Verschwiegenheitspflicht an eine andere Behörde weitergegeben worden sind. Für derartige Weitergaben gilt der Grundsatz der Zweckbindung. Dieser Grundsatz darf nicht weit aber auch nicht dem Schutzinteresse widersprechend eng ausgelegt werden. So werden beispielsweise Daten, die anlässlich eines Arbeitsunfalls angefallen sind, von der Unfallversicherung auch an die Rentenversicherung weitergegeben werden können, wenn sie für eine etwaige Rentengewährung von Bedeutung sein sollten. Maßgeblicher Zweck ist in diesem Falle die Realisierung der gegenüber der Sozialversicherung bestehenden Ansprüche des Bürgers.

Absatz 1 Satz 2 hat die Weitergabe anderer personenbezogener Daten zum Gegenstand. Durch die Bestimmung wird gewährleistet, daß der zwischen den Behörden und Stellen aller öffentlichen Bereiche geübte Datenaustausch, der sich in der Vergangenheit bewährt und als für die Wirksamkeit der öffentlichen Verwaltung notwendig erwiesen hat, durch das Gesetz nicht eingeschränkt werden soll, sofern die Zulässigkeitsvoraussetzungen erfüllt sind. Wegen näherer Einzelheiten zu diesen Voraussetzungen wird auf die Begründung zu § 6 Abs. 1 verwiesen.

Absatz 2 stellt in Ergänzung des Absatzes 1 klar, daß die Weitergabe personenbezogener Daten durch die unter den zweiten Abschnitt fallenden Behörden und Stellen im Rahmen des Absatzes 1 auch an Stellen der öffentlich-rechtlichen Religionsgesellschaften zulässig ist, sofern sichergestellt ist, daß die Daten bei dem Empfänger ausreichend, das heißt, im Sinne dieses Gesetzes, geschützt werden. Damit wird dem Umstand Rechnung getragen, daß die Kirchen auch aus dem öffentlichen Bereich die für die Erfüllung ihrer Aufgaben erforderlichen Daten erhalten **sollen**.

Absatz 3 Satz 1 fordert für den Fall, daß automatisierte Datenübermittlungswege bestehen – etwa durch Datenfernübertragung –, geeignete Vorkehrungen, die sicherstellen, daß die Datenweitergaben nur im zulässigen Umfang erfolgen. Nach dem derzeitigen Stand der Entwicklung auf diesem Gebiet gibt es außer den herkömmlichen Sicherheitsmaßnahmen eine Vielzahl von anlagegebundenen und programmierten Sperrungen und Verschlüsselungen, die einen hinreichenden Schutz gegen den unbefugten Zugriff auf Daten bieten. Als solche Vorkehrungen werden auch regelmäßige Überprüfungen der Anwendungsprogramme auf deren Übereinstimmung mit den materiellen Schutzvorschriften zu gelten haben.

Während Absatz 3 Satz 1 Vorsorgemaßnahmen vorschreibt, soll Absatz 3 Sätze 2 und 3 Kontrollen ermöglichen. Für den Fall selbsttätiger Datenweitergaben durch öffentliche Stellen, die im Rahmen eines vorher festgelegten periodischen Mitteilungsdienstes stattfinden, kann eine Überprüfung der Rechtmäßigkeit der Datenweitergaben anhand der Programmdokumentation und weiterer Unterlagen erfolgen. Dies ist aber nicht in gleichem Umfang möglich, wenn Daten auf Abruf bereitstehen und bei Bedarf selbsttätig dem Empfänger zufließen. Für diese Fälle wird deshalb die Führung eines Protokolls vorgeschrieben, damit durch diese zusätzliche Maßnahme die nachträgliche Kontrolle voll gewährleistet bleibt.

Zu § 8 – Datenweitergabe an Dritte

Absatz 1 Satz 1 hat die Weitergabe personenbezogener Daten durch Behörden an außerhalb ihres Bereichs stehende Dritte, sofern die Daten einem Berufs- oder besonderen Amtsgeheimnis unterliegen, zum Gegenstand. Allerdings kann im Falle einer Weitergabe an Dritte der Zweckbestimmungsgrundsatz nicht als Maßstab für die Zulässigkeit der Weitergabe dienen. Hier muß die weitergebende Behörde vielmehr prüfen, ob die zur Verschwiegenheit verpflichtete Person, von der sie die Daten erhalten hat, diese unter den gegebenen Voraussetzungen weitergeben dürfte. Die Weitergabe anderer personenbezogener Daten ist nach Satz 2 grundsätzlich an die gleichen Zulässigkeitsvoraussetzungen geknüpft wie die Speicherung und die interne Weitergabe. Darüber hinaus ist sie in den Fällen zulässig, in denen der Dritte ein berechtigtes

Interesse an dem Empfang der Daten glaubhaft macht und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden, was z. B. nicht der Fall sein dürfte, wenn neben freien Daten Angaben über die Zugehörigkeit zu einer Personengruppe weitergegeben werden. Ferner soll der immer wichtiger werdende Datenaustausch mit ausländischen sowie über- und zwischenstaatlichen Behörden und Stellen nach Maßgabe der gesetzlichen und durch Vereinbarung eingegangenen Verpflichtungen zulässig sein.

Die in Absatz 2 genannten personenbezogenen Daten sind im allgemeinen offenkundig. Da über sie erfahrungsgemäß am häufigsten Auskunft durch Dritte verlangt wird, dient die Vorschrift der leichteren Handhabbarkeit des Gesetzes und der Entlastung der datenverarbeitenden Behörden und Stellen. Sie findet auch im Rahmen einer Reihe von weiteren Vorschriften dieses Gesetzes entsprechende Anwendung.

Die Weitergabe personenbezogener Daten an Dritte ist nach Absatz 3 ausnahmslos untersagt, wenn zu befürchten ist, daß dem Betroffenen dadurch schwerwiegende rechtswidrige Nachteile erwachsen können.

Nach Absatz 4 gelten die in § 7 Abs. 3 enthaltenen grundsätzlichen Vorschriften über den Einsatz technischer Vorkehrungen und Maßnahmen bei Anwendung der automatischen Datenverarbeitung hier entsprechend.

Zu § 9 – Datenveränderung

In Absatz 1 wird geregelt, unter welchen Voraussetzungen personenbezogene Daten verändert werden dürfen. Die Verpflichtung zur Veränderung ist demgegenüber Gegenstand der Regelung in § 12 Abs. 1; der Hinweis in Satz 2 auf § 12 Abs. 1 stellt dies klar. Veränderungen sind immer dann gegeben, wenn das personenbezogene Datum einen anderen Inhalt bekommen hat. Das kann geschehen etwa durch Hinzufügen neuer Daten, durch teilweise Löschung oder durch Verknüpfung mit anderen personenbezogenen Daten. Die vollständige Löschung eines Datums, also dessen ersatzlose Beseitigung, ist keine Veränderung im Sinne dieser Vorschrift; sie wird in § 12 Abs. 2 geregelt.

Absatz 2 enthält eine technisch-organisatorische Grundsatzvorschrift zur Verhinderung mißbräuchlicher Veränderungen (z. B. Verfälschungen) von personenbezogenen Daten beim Einsatz der automatischen Datenverarbeitung. Sie wird durch die Bestimmungen einer künftigen Rechtsverordnung nach § 4 Abs. 2 noch zu konkretisieren sein.

Zu § 10 – Veröffentlichung über die gespeicherten Daten

Diese Vorschrift ist im Zusammenhang mit dem in § 11 geregelten Auskunftsrecht des Bürgers zu

sehen. Dieser könnte sein Recht in zahlreichen Fällen nicht ausüben, weil ihm nicht bekannt ist, welche öffentliche Stelle ihn betreffende Daten speichert.

§ 10 ermöglicht es dem Bürger nunmehr, sich über die Art der von einer Stelle gespeicherten Daten sowie über den betroffenen Personenkreis zu unterrichten und daraus zu ersehen, ob ihn betreffende personenbezogene Daten darunter sein könnten. Er ist dann in der Lage, von seinem Auskunftsrecht gezielt Gebrauch zu machen. Im übrigen werden diese Veröffentlichungen die Datenverarbeitung in der öffentlichen Verwaltung für den Bürger durchsichtig machen und unberechtigtes Mißtrauen ausschließen sowie eine fruchtbare öffentliche Diskussion über die Notwendigkeit der Speicherung auslösen können. Die Entbindung der in Satz 2 genannten Behörden von der Bekanntmachungspflicht ergibt sich aus deren besonderer Aufgabenstellung.

Zu § 11 – Auskunftserteilung

Absatz 1 legt der Behörde oder sonstigen Stelle die Verpflichtung auf, dem Betroffenen über die zu seiner Person gespeicherten Daten Auskunft zu erteilen. Um die mit dieser Auskunftspflicht verbundene Belastung im Rahmen des Möglichen und Erträglichen zu halten und im Interesse des Staatsbürgers, der sonst von einer Flut von Auskunftschreiben überschwemmt werden würde, wird die Auskunft nur auf Antrag erteilt. In dem Antrag ist die Art der gewünschten personenbezogenen Daten näher zu bezeichnen; dadurch kann die Auskunft – vor allem bei großen Behörden mit umfangreichen und vielfältigen Datenbeständen – beschleunigt werden. Von der sehr personal- und kostenaufwendigen Ausdehnung der Auskunftspflicht auf die Datenweitergaben wurde abgesehen, weil der damit verfolgte Schutzzweck durch das Gesetz auch ohne eine solche Regelung erreicht wird (vgl. Allgemeine Begründung Nr. 3.9.7). Die Auskunft kann durch Einsichtnahme in die Karteien, durch Übersendung einer Abschrift oder eines Speicherauszugs oder dergl. erfolgen. Für das nähere Verfahren sind die spezialgesetzlichen Regelungen (§ 37) maßgebend, im übrigen bestimmt es die speichernde Stelle nach pflichtgemäßen Ermessen. Danach kann es z. B. geboten sein, bestimmte Gesundheitsdaten dem Betroffenen durch einen Arzt eröffnen zu lassen.

Die Absätze 2 und 3 enthalten Regelungen für das Entfallen der Auskunftspflicht. Es handelt sich dabei vor allem um Fälle aus dem Bereich der staatlichen Sicherheit und der Verbrechensbekämpfung, in denen die Verweigerung der Auskunft geboten ist, um die Arbeit der zuständigen Behörden vor schweren, ihre Wirksamkeit in Frage stellenden Beeinträchtigungen zu bewahren und Nachteile für die öffentliche Sicherheit und Ordnung oder sonst für das öffentliche Wohl zu vermeiden. Diese Nachteile wären insbesondere zu befürchten, wenn ein Zwang zur Erteilung von Auskünften durch die einschlä-

gigen Behörden an – als Träger verfassungsfeindlicher Bestrebungen oder als Mitarbeiter fremder Nachrichtendienste – überwachte oder in Strafverfolgung befindliche Personen darüber bestünde, ob und welche Informationen über sie gespeichert werden. Darüber hinaus entfällt die Auskunftspflicht, sofern die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, z. B. wegen der überwiegenden berechtigten Interessen einer dritten Person geheimgehalten werden müssen oder wenn sie sich auf die Weitergabe an eine der in § 10 Satz 2 genannten Behörden bezieht.

Die Auskunftsverpflichtung entfällt nach Absatz 2 für die in § 10 Satz 2 genannten Behörden wegen ihrer besonderen Aufgabenstellung generell, während sie nach Absatz 3 von allen übrigen Behörden und öffentlichen Stellen im Einzelfall besonders geprüft werden muß.

Nach Absatz 4 ist die Auskunft als besondere Leistung der Verwaltung gebührenpflichtig. Die Bundesregierung regelt das Nähere in einer Rechtsverordnung, die der Zustimmung des Bundesrates bedarf. Das gilt insbesondere für die gebührenpflichtigen Tatbestände, die Ausnahmen von der Gebührenpflicht sowie die Höhe der Gebühr.

Zu § 12 – Berichtigung, Löschung und Sperrung von Daten

Absatz 1 bestimmt die Voraussetzungen für die Verpflichtung zu einer Berichtigung der personenbezogenen Daten. Die Berichtigung besteht in der Regel in einer Veränderung (wegen dieses Begriffs vgl. Begründung zu § 9 Abs. 1). Läßt sich weder die Richtigkeit noch die Unrichtigkeit der gespeicherten Daten feststellen, werden diese von der Verwaltung aber gleichwohl benötigt, so sind sie mit einem entsprechenden Hinweis zu versehen. Dadurch soll erreicht werden, daß diese non-liquet-Fälle mit der nötigen Vorsicht behandelt werden.

Absatz 2 nennt die Voraussetzung für die Verpflichtung zur Löschung von Daten, nämlich die Unzulässigkeit der Speicherung. Gemeint ist damit das Unkenntlichmachen der Daten (§ 3 Abs. 2 Nr. 5), z. B. durch deren ersatzlose Beseitigung. Daneben wird in Absatz 3 die Sperrung für die Fälle vorgeschrieben, in denen der Zweck der Speicherung weggefallen ist, die Daten für die Abwicklung der Geschäfte also nicht mehr benötigt werden. Die Sperrung hat zur Folge, daß die Daten grundsätzlich nicht mehr genutzt werden dürfen mit Ausnahme einiger bestimmter Fälle, in denen die Daten zu einem späteren Zeitpunkt zu bestimmten Zwecken unbedingt wieder gebraucht werden.

Zu § 13 – Verarbeitung personenbezogener Daten im Auftrage anderer Behörden und sonstiger Stellen

Diese Vorschrift enthält den Grundsatz, daß eine Behörde, die personenbezogene Daten durch andere

Stellen (z. B. Behörden mit freier Datenverarbeitungskapazität oder gemeinsame Rechenzentren) speichern oder verarbeiten läßt, für den Schutz dieser Daten verantwortlich bleibt. Ohne Zustimmung der auftraggebenden Behörde oder sonstigen Stelle dürfen personenbezogene Daten nicht weitergegeben, verändert oder gelöscht werden. Die beauftragte Stelle ist nach Satz 2 jedoch für die Durchführung technischer und organisatorischer Maßnahmen zur Verhinderung von Mißbräuchen verantwortlich.

Zu § 14 – Durchführung des Datenschutzes in der Bundesverwaltung

Diese Vorschrift soll die Durchführung des Datenschutzes sicherstellen. Dabei wurde von der Einführung einer institutionalisierten Fremdkontrolle abgesehen und versucht, das Prinzip der Selbstverantwortlichkeit und Selbstkontrolle in wirkungsvoller Weise zu verfolgen. Auf die Ausführungen im Allgemeinen Teil der Begründung (Nr. 3.8) wird insoweit verwiesen. Die Regelungen dieser Vorschrift beschränken sich auf die Bundesverwaltung. In die innere Organisation anderer Verwaltungen soll hier nicht eingegriffen werden. Es wäre aber wünschenswert, wenn die Länder ähnliche Regelungen treffen würden.

In Satz 1 wird den obersten Bundesbehörden sowie den übrigen dort genannten Stellen vorgeschrieben, jeweils für ihren Geschäftsbereich die Ausführung des Gesetzes sowie anderer einschlägiger Rechtsvorschriften über den Datenschutz sicherzustellen. Das soll durch geeignete Maßnahmen geschehen, die nach den Besonderheiten des jeweiligen Geschäftsbereichs zum Teil auch unterschiedlich gestaltet werden können. Einige besonders wichtige Maßnahmen werden schwerpunktmäßig in Satz 2 Nummern 1 und 2 vorgeschrieben. Die Durchführung dieser und weiterer Maßnahmen wird am besten dadurch gesichert werden können, daß für jeden Geschäftsbereich und bei obersten Bundesbehörden mit großem Geschäftsbereich auch für einschlägige Bundesabteilungen und für die nachgeordneten Behörden ein für den Datenschutz zuständiger Beamter bestellt wird. Der Begriff „Geschäftsbereich“ ist hier im engeren Sinne zu verstehen, dazu gehören aber auch die nachgeordneten Behörden und Stellen.

Zu § 15 – Allgemeine Verwaltungsvorschriften

Diese Vorschrift sieht den Erlass allgemeiner Verwaltungsvorschriften vor, die die Ausführung dieses Gesetzes regeln. Diese Regelungen sollen möglichst konkret sein und sich auf die besonderen Verhältnisse und die sich daraus ergebenden Erfordernisse für den Datenschutz in möglichst kleinen und überschaubaren Verwaltungsbereichen beziehen.

Unter diesem Gesichtspunkt wäre die wohl wirksamste Lösung, jede datenverarbeitende Behörde oder sonstige Stelle zum Erlass einer Dienstanwei-

sung zu verpflichten, in der die datenschutzrelevanten Verwaltungs- und Datenverarbeitungsvorgänge in allen Einzelheiten geregelt werden können. Da eine solche Bestimmung rechtlich problematisch wäre, wird der – nach Artikel 86 GG zulässige – Weg des Erlasses von allgemeinen Verwaltungsvorschriften der obersten Bundesbehörden für ihren jeweiligen Bereich gegangen. Auch auf diese Weise ist es möglich, die Regelungen des Gesetzes für die einschlägigen Bereiche der obersten Bundesbehörden auch in nachgeordneten Behörden zu konkretisieren.

Die Möglichkeit, in allgemeine Verwaltungsvorschriften, die zu einem Verwaltungsbereich erlassen sind (z. B. VV zum Bundesbeamtengesetz), dem Datenschutz dienende Bestimmungen aufzunehmen, bleibt daneben unberührt.

Zu dritten Abschnitt –

Datenverarbeitung nicht öffentlicher Stellen für eigene Zwecke

Zu § 16 – Anwendungsbereich

Nach dieser Bestimmung gelten die Vorschriften des dritten Abschnitts für die Datenverarbeitung im nicht-öffentlichen Bereich für interne Zwecke. Sie gelten mit Ausnahme der in Absatz 1 Satz 2 genannten, am wirtschaftlichen Wettbewerb teilnehmenden Stellen nicht für juristische Personen des öffentlichen Rechtes oder Einrichtungen davon, auch wenn sie keine öffentlichen Aufgaben erfüllen; sie gelten aber für juristische Personen des privaten Rechtes, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder ihr die Mehrheit der Stimmen zusteht. Die Vorschriften dieses Abschnitts sind gerichtet an natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechtes, die keine eigene Rechtspersönlichkeit besitzen, aber auch nicht Teile von juristische Personen sind (z. B. nicht rechtsfähiger Verein, offene Handelsgesellschaft).

Maßgebend für die Zugehörigkeit zum Anwendungsbereich dieses Abschnitts ist der Zweck der Datenverarbeitung. Die Vorschriften dieses Abschnitts gelten in allen denjenigen Fällen, in denen die Datenverarbeitung nicht als Selbstzweck ausgeübt wird – solche Fälle werden im vierten Abschnitt geregelt –, sondern als Hilfsmittel zur Optimierung der Erfüllung der Geschäftszwecke oder Ziele des Anwenders, die nicht in der Speicherung oder Weitergabe oder der sonstigen Verarbeitung von personenbezogenen Daten bestehen. Es handelt sich also hauptsächlich um Daten über Lieferanten, Kunden, Klienten, Patienten, Arbeitnehmer, Mitglieder usw., die von Wirtschaftsbetrieben, Dienstleistungsunternehmen, Krankenhäusern, Arbeitgebern, Verbänden usw. verarbeitet werden.

Absatz 2 stellt sicher, daß die Daten auch dann nach diesem Gesetz geschützt bleiben, wenn sie durch andere Stellen im Auftrage gespeichert und verarbeitet werden. Normadressat der Vorschriften dieses Abschnittes ist der Auftraggeber, nicht die beauftragte Stelle.

Absatz 3 schließt an § 5 Abs. 5 an und stellt klar, daß die sog. beliebigen Unternehmer nicht unter den dritten Abschnitt fallen.

Zu § 17 – Datenspeicherung

In dieser Vorschrift wird die Datenspeicherung, also der Eingang der personenbezogenen Daten in das interne System der Datenverarbeitung geregelt. Sie ist danach, abgesehen von der Zustimmung des Betroffenen oder auf Grund einer Rechtsvorschrift (§ 2 Abs. 3), zulässig, wenn sie sich im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit der Person, auf die sich die Daten beziehen, hält. Sie ist auch zulässig, wenn sie z. B. außerhalb von Vertrags- oder vertragsähnlichen Vertrauensverhältnissen, zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden können.

Zu § 18 – Datenweitergabe

Die Vorschrift regelt die Fälle der Weitergabe personenbezogener Daten an Dritte außerhalb des Geschäftsbereichs der datenverarbeitende Stelle. Für Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, gilt eine Regelung analog derjenigen in § 8 Abs. 1 Satz 1. Für die Weitergabe anderer personenbezogener Daten gelten die gleichen Voraussetzungen wie für die Speicherung (§ 17). Die Regelung der Weitergabe in dieser Vorschrift gilt nicht für die Fälle, in denen sich die Weitergabe auf die in § 8 Abs. 2 genannten, meist ohnehin schon offenkundigen Informationen beschränkt. Die Vorschriften in § 7 Abs. 3 über die Einführung technischer und organisatorischer Vorkehrungen und Maßnahmen gegen unzulässige Datenweitergaben und Abrufe durch Unbefugte gelten entsprechend.

Zu § 19 – Datenveränderung

Diese Vorschrift nennt die Voraussetzungen, unter denen personenbezogene Daten verändert werden dürfen, während die Verpflichtung zur Veränderung in § 21 Abs. 1 geregelt wird (vgl. Verweisung in Satz 2). Die vollständige Lösung personenbezogener Daten ist keine Veränderung im Sinne dieser Vorschrift; sie wird in § 21 Abs. 2 geregelt. Wegen der Bestimmung des Begriffs der Veränderung wird im übrigen auf die Begründung zu § 9 Abs. 1 Bezug genommen.

Nach Satz 3 gilt hier die in § 9 Abs. 2 enthaltene technisch-organisatorische Grundsatzvorschrift zur

Verhinderung mißbräuchlicher Veränderungen von personenbezogenen Daten beim Einsatz der automatischen Datenverarbeitung entsprechend.

Zu § 20 – Auskunftserteilung

Absatz 1 erfaßt die Fälle, in denen die Speicherung außerhalb von Vertrags- oder vertragsähnlichen Vertrauensverhältnissen oder sonst ohne Wissen des Betroffenen erfolgte. In diesen Fällen muß er über die Tatsache der Speicherung unterrichtet werden, um überhaupt von seinen weiteren Rechten Gebrauch machen zu können (vgl. dazu auch die Allgemeine Begründung Nr. 3.9.7). Die Benachrichtigungspflicht entfällt, wenn der Betroffene anderweitig Kenntnis von der Speicherung erlangt hat. Dieser Fall ist z. B. dann gegeben, wenn dem Betroffenen bei Vertragsabschluß mitgeteilt wird, daß beabsichtigt sei, ihn betreffende personenbezogene Daten bei Vorliegen bestimmter Voraussetzungen künftig zu speichern.

Absatz 2 gibt dem Betroffenen ein Recht auf Auskunft über die zu seiner Person gespeicherten Daten. Die Verpflichtung des Betroffenen, die Art der gewünschten Informationen näher zu bezeichnen, soll vor allem bei Unternehmen usw. mit großen und vielfältigen Datenbeständen (z. B. Kunden-, Lieferanten- und Arbeitnehmerdateien) die Auskunftserteilung beschleunigen helfen. Von der sehr personal- und kostenaufwendigen Ausdehnung der Auskunftspflicht auf die Datenweitergaben wurde abgesehen, weil der damit verfolgte Schutzzweck durch das Gesetz auch ohne eine solche Regelung erreicht wird (vgl. Allgemeine Begründung Nr. 3.9.7).

Das in Absatz 3 vorgesehene Entgelt soll dem Unternehmer die durch die Auskunftserteilung entstandenen Unkosten ersetzen, ohne ihm einen Gewinn zu verschaffen. Die Ausnahmegvorschrift in Satz 2 trifft vor allem die Fälle, in denen der Betroffene durch die Auskunft Kenntnis davon erhält, daß ihn betreffende Daten berichtigt oder gelöscht werden müssen. Hier würde eine Kostenbelastung des Betroffenen unbillig erscheinen.

Absatz 4 enthält Regelungen für das Entfallen der Auskunftserteilung und deshalb auch der Benachrichtigung nach Absatz 1. Es handelt sich dabei zunächst um Fälle, in denen die Auskunftserteilung Geschäftszwecke oder Ziele der speichernden Stelle erheblich gefährden würde; dabei ist jedoch die Gefährdung gegen die gegenüberstehenden berechtigten Interessen des Betroffenen abzuwägen. Im übrigen entfällt die Auskunftsverpflichtung immer dann, wenn es zur Vermeidung von Nachteilen für die öffentliche Sicherheit oder Ordnung geboten oder sonst für das öffentliche Wohl unerlässlich ist oder wenn die Auskünfte geheimhaltungsbedürftig sind. Hierwegen wird auf die Begründung zu § 10 Abs. 2 Bezug genommen. Diese Regelung ist u. a. dann von Bedeutung, wenn Rechtspersonen des privaten Rechts für die öffentliche Hand tätig werden.

Zu § 21 – Berichtigung, Löschung und Sperrung von Daten

In Absatz 1 werden die Voraussetzungen für die Verpflichtung zu einer Berichtigung der personenbezogenen Daten bestimmt. Die Berichtigung besteht in der Regel in einer Veränderung. Voraussetzung für die Berichtigung ist, daß die Daten unrichtig gespeichert sind. Im übrigen wird auf die Begründung zu § 12 Abs. 1 verwiesen.

Absatz 2 regelt in Satz 1 die Berechtigung und in Satz 2 die Verpflichtung zur Löschung. In beiden Fällen steht die Wahrung der Interessen des Betroffenen im Vordergrund der Regelung.

Absatz 3 bestimmt die Voraussetzungen für eine Sperrung personenbezogener Daten. Die Regelung entspricht derjenigen des § 12 Abs. 3.

Zu § 22 – Durchführung des Datenschutzes

Durch diese Vorschrift soll die Durchführung des Datenschutzes im Anwendungsbereich des dritten Abschnitts sichergestellt werden. Unter dem Gesichtspunkt der Freiheit der Berufsausübung und der Freiheit im wirtschaftlichen Verkehr wurde von der Einführung einer institutionalisierten Fremdkontrolle abgesehen. Vielmehr soll das Prinzip der Selbstverantwortlichkeit und Selbstkontrolle in für den Datenschutz wirkungsvoller Weise verfolgt werden. Auf die Ausführungen im Allgemeinen Teil der Begründung Nr. 3.8 wird verwiesen.

In Absatz 1 wird den Stellen, die im Anwendungsbereich des dritten Abschnittes Datenverarbeitung betreiben, die Bestellung eines Beauftragten für den Datenschutz vorgeschrieben, der die Durchführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz in ihrem Geschäftsbereich sicherzustellen hat. Er ist hinsichtlich dieser Aufgaben dem Inhaber oder dem gesetzlich oder verfassungsmäßig berufenen Leiter unmittelbar unterstellt; damit soll seine Effektivität gesteigert werden. Diese Regelung gilt, wenn die Datenverarbeitung automatisch, insbesondere elektronisch betrieben wird und hierbei in der Regel mindestens fünf Arbeitnehmer ständig beschäftigt sind, sowie in den Fällen konventioneller Datenverarbeitung bei ständiger Beschäftigung von wenigstens 20 Arbeitnehmern.

In Absatz 2 werden einige besonders wichtige Aufgaben des nach Absatz 1 zu bestellenden Beauftragten für den Datenschutz schwerpunktmäßig genannt.

Zum vierten Abschnitt –

Geschäftsmäßige Datenverarbeitung
nicht-öffentlicher Stellen für Dritte

Zu § 23 – Anwendungsbereich

Die Vorschriften des vierten Abschnittes gelten nach dieser Bestimmung für die Datenverarbeitung im nicht-öffentlichen Bereich, soweit Personen, Gesell-

schaften oder andere Personenvereinigungen des privaten Rechts personenbezogene Daten geschäftsmäßig für Dritte verarbeiten. Es handelt sich dabei um drei Fallgruppen, die unterschiedlich zu behandeln sind. Sie werden in Absatz 1 Nr. 1 bis 3 umschrieben. Maßgebendes Kriterium für die Anwendung des vierten Abschnittes ist die Zweckbestimmung der Datenverarbeitung für Dritte. Sofern die Daten primär für eigene Zwecke verarbeitet und daneben auch an Dritte weitergegeben werden, handelt es sich um Fälle des dritten Abschnittes (vgl. die Begründung zu § 16). Soweit Stellen, deren Geschäftszweck die Datenverarbeitung für Dritte ist (z. B. Auskunfteien), auch Datenverarbeitung für interne Zwecke betreiben (z. B. mit Daten über Kunden oder Mitarbeiter), kommt der dritte Abschnitt zur Anwendung.

Nach Absatz 1 Nr. 1 gelten die §§ 24 bis 27, 30 und 31 dieses Abschnittes für die dort genannten Personen und Stellen, die personenbezogene Daten geschäftsmäßig zum Zweck der Weitergabe in Dateien speichern und als solche weitergeben. Eine Veränderung oder sonstige Verarbeitung dieser Informationen steht der Anwendbarkeit des Absatzes 1 dann nicht entgegen, wenn deren Qualität als personenbezogene Daten (vgl. hierzu die Legaldefinition in § 3 Abs. 1) dadurch nicht verlorengeht. Hierunter fallen z. B. Auskunfteien und Detekteien.

Nach Absatz 1 Nr. 2 gelten die §§ 28, 30 und 31 für die Stellen, die personenbezogene Daten geschäftsmäßig zum Zwecke der Veränderung und Weitergabe in Dateien speichern, sie so verändern (insbesondere anonymisieren oder aggregieren), daß ihre Qualität als personenbezogene Daten verlorengeht und diese neuen Daten weitergeben. Dazu gehören z. B. Markt- oder Meinungsforschungsinstitute.

Nach Absatz 1 Nr. 3 gelten die §§ 29 bis 31 für die Stellen, die personenbezogene Daten geschäftsmäßig für andere Personen und Stellen in Dateien speichern, verändern oder sonst verarbeiten, das sind z. B. Lohnrechenzentren; ausgenommen sind die funktionell der öffentlichen Hand zugehörigen Stellen, auch wenn sie in privater Rechtsform betrieben werden.

Zu § 24 – Datenspeicherung und -weitergabe

In Absatz 1 wird die Zulässigkeit der Datenspeicherung geregelt. Sie ist dann gegeben, wenn dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden können.

Absatz 2 regelt die Zulässigkeit der Weitergabe der personenbezogenen Daten durch den Unternehmer. Zunächst hängt die Zulässigkeit von einem berechtigten Interesse des Empfängers an der Kenntnis der personenbezogenen Daten ab. Ein berechtigtes Interesse kann vor allem dann gegeben sein, wenn die Kenntnis der Daten im Zusammenhang mit Rechtsverhältnissen des Empfängers, insbesondere mit einem Kredit-, Versicherungs- oder Dienstvertrag erforderlich ist. Der Empfänger muß sein be-

rechtiges Interesse dem Unternehmer glaubhaft darlegen, was in der Regel durch Vorlage entsprechender Urkunden, bei langjährigen geschäftlichen Beziehungen zwischen Unternehmer und Empfänger aber auch durch bloßen Hinweis auf den Geschäftsvorgang des Empfängers geschehen kann. Der Unternehmer hat die Gründe für das Vorliegen eines berechtigten Interesses und die Mittel für ihre Glaubhaftmachung schriftlich oder in anderer geeigneter Weise festzuhalten. Die technische Grundsatzbestimmung des § 7 Abs. 3 findet entsprechend Anwendung.

Nach Absatz 3 ist abweichend von Absatz 2 Satz 1 die Weitergabe auch ohne Glaubhaftmachung eines berechtigten Interesses zulässig, wenn sie sich auf die in § 8 Abs. 2 genannten freien Daten sowie auf eine Angabe über die Zugehörigkeit des Betroffenen zu einer bestimmten Personengruppe beschränkt und auch insoweit schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden können. Durch diese Vorschrift soll den Bedürfnissen der Werbewirtschaft auf eine mit dem Datenschutzgedanken verträgliche Weise Rechnung getragen werden.

Zu § 25 – Datenveränderung

In dieser Bestimmung werden die Voraussetzungen festgelegt, unter denen personenbezogene Daten verändert werden dürfen. Demgegenüber bestimmt § 27 Abs. 1, unter welchen Voraussetzungen Veränderungen vorgenommen werden müssen; hierauf weist die Bezugnahme auf § 27 Abs. 1 in Satz 2 hin. Die vollständige Löschung personenbezogener Daten ist keine Veränderung im Sinne dieser Vorschrift. Sie wird in § 27 Abs. 3 geregelt.

Nach Satz 3 gilt hier die in § 9 Abs. 2 enthaltene technisch-organisatorische Grundsatzbestimmung zur Verhinderung von mißbräuchlichen Veränderungen der personenbezogenen Daten beim Einsatz der automatischen Datenverarbeitung entsprechend.

Zu § 26 – Auskunftserteilung

Nach Absatz 1 hat der Unternehmer den Betroffenen, sobald erstmals zu seiner Person gespeicherte Daten weitergegeben worden sind, über die Tatsache dieser Speicherung zu benachrichtigen, es sei denn, dieser hat auf andere Weise von der Speicherung Kenntnis erlangt oder die Weitergabe beschränkte sich auf freie Daten sowie auf eine Angabe über die Zugehörigkeit des Betroffenen zu einer Personengruppe. Diese Benachrichtigung ist zumeist Voraussetzung für das in Absatz 2 geregelte Auskunftsrecht des Betroffenen. Anders als in den Fällen des dritten Abschnittes hat der Betroffene hier ohne die Benachrichtigung in aller Regel keine Kenntnis davon, daß Daten über ihn zum Zweck der Weitergabe gespeichert werden. Ausnahmefälle – z. B. die Bank gibt ihrem Kreditkunden von der Datenweitergabe an die Schufa Kenntnis – werden in Satz 1 berücksichtigt (vgl. dazu auch den Allgemeinen Teil der Begründung Nr. 3.9.7).

Absatz 2 gibt dem Betroffenen ein Recht auf Auskunft über die zu seiner Person gespeicherten Daten. Die Auskunft wird grundsätzlich schriftlich erteilt. Das Gesetz braucht keine Regelungen zu treffen, um Mißbräuche zu verhüten, die vom Betroffenen mit einer schriftlich erteilten Auskunft über die zu seiner Person, etwa bei einer Auskunft, gespeicherten Daten getrieben werden könnten. Hiergegen kann vom Unternehmer durch Beifügung eines Vermerks, wonach die Auskunft nur zur Unterrichtung des Betroffenen persönlich bestimmt sei, mit Angabe des Ausstelltages oder durch ähnliche Maßnahmen selbst Vorsorge getroffen werden, ohne daß das Auskunftsrecht des Betroffenen geschmälert werden müßte.

Wegen des in Absatz 3 vorgesehenen Entgelts vgl. die Begründung zu § 20 Abs. 3.

In Absatz 4 sind für ähnliche Fälle wie in §§ 11 und 21 Ausnahmen von der Benachrichtigungspflicht und dem Auskunftsrecht vorgesehen.

Zu § 27 – Berichtigung, Löschung und Sperrung von Daten

Absatz 1 bestimmt die Voraussetzungen für die Verpflichtung zu einer Berichtigung der beim Unternehmer gespeicherten personenbezogenen Daten.

Danach sind diese Daten zu berichtigen, wenn sie unrichtig gespeichert sind. Läßt sich ein Streit über die Richtigkeit oder Unrichtigkeit nicht beheben, kann der Betroffene verlangen, daß den zu seiner Person gespeicherten Daten ein Hinweis auf diese Ungewißheit oder seine eigene Gegendarstellung beigefügt wird.

In Absatz 2 wird vorgeschrieben, daß die Berichtigung, der Hinweise oder die Gegendarstellung den bisherigen Empfängern der betreffenden Daten zur Kenntnis zu bringen sind. Auch bei künftigen Weitergaben sind Hinweis und Gegendarstellung stets beizufügen. Durch diese Regelung wird die Berichtigungspflicht nach Absatz 1 auf wirkungsvolle Weise ergänzt.

Absatz 3 Satz 1 nennt die Voraussetzungen, unter denen personenbezogene Daten gelöscht werden können. Nach Satz 2 sind sie zu löschen, wenn ihre Speicherung unzulässig war. In Anlehnung an den Grundgedanken der §§ 107 Abs. 2 KO, § 915 ZPO ist in Absatz 4 außerdem bestimmt, daß sie auf Verlangen des Betroffenen nach Ablauf von fünf Jahren seit ihrer Einspeicherung zu sperren sind.

Zu § 28 – Verarbeitung personengezogener Daten zum Zwecke der Weitergabe in anonymisierter Form

In dieser Vorschrift werden nähere Regelungen für die in § 23 Abs. 1 Nr. 2 genannten Stellen, z. B. Markt- und Meinungsforschungsinstitute, getroffen. Die Vorschrift geht davon aus, daß diese Unterneh-

men die als Rohstoff für ihre Untersuchungen und Auswertungen benötigten personenbezogenen Daten nur mit Zustimmung des Betroffenen oder auf Grund einer Rechtsvorschrift verarbeiten dürfen (§ 2 Abs. 3). Nach Wegfall des Speicherungszwecks, spätestens am Ende des fünften Jahres nach Einspeicherung, sind die Daten zu anonymisieren. Die Identifizierungsmerkmale sind gesondert zu speichern, sie dürfen mit den anonymisierten Daten nur in bestimmten Fällen, z. B. bei Langzeiterhebungen, wieder zusammengeführt werden. Bei der automatischen Datenverarbeitung sind nach Absatz 2 Vorkehrungen zu treffen, daß personenbezogene Daten nicht mißbräuchlich weitergegeben oder abgerufen werden können.

Zu § 29 – Verarbeitung personenbezogener Daten im Auftrag Dritter

Satz 1 regelt die datenschutzrelevanten Tätigkeiten der in § 23 Abs. 1 Nr. 3 genannten Stellen. Es handelt sich dabei um solche Stellen, die die geschäftsmäßige Speicherung, Veränderung und sonstige Verarbeitung personenbezogener Daten im fremden Auftrag betreiben (z. B. Lohnrechenzentren). Sie sollen die vom Auftraggeber gelieferten personenbezogenen Daten nur mit dessen Zustimmung weitergeben, verändern oder löschen dürfen, sind jedoch nach Absatz 2 für die Durchführung technischer und organisatorischer Maßnahmen zur Verhinderung von Mißbräuchen verantwortlich.

Zu § 30 – Meldepflichten

Diese Vorschrift – wie auch § 31 – dient der Sicherstellung der Durchführung des Datenschutzes im Anwendungsbereich des vierten Abschnitts. Mit Rücksicht auf die Besonderheiten der in diesem Abschnitt geregelten Unternehmen – geschäftsmäßiger Umgang mit fremden personenbezogenen Daten – war die Überwachung und Kontrolle der Durchführung des Datenschutzes durch Aufsichtsbehörden vorzusehen. Diesem Zweck dient die Anmeldung zu dem bei der zuständigen Aufsichtsbehörde geführten Register über diese Unternehmen. Bei der Anmeldung sind die Angaben zu machen, die für die Kontrolle und Überwachung von Bedeutung sind. Anmeldepflichten und Registern nach gewerberechtl. Vorschriften liegen andere Zielsetzungen zugrunde, sie bleiben nach § 31 Abs. 4 unberührt.

Zu § 31 – Aufsichtsbehörde

Die Vorschrift regelt Aufgaben und Befugnisse der nach Landesrecht zuständigen Aufsichtsbehörde (zu deren Zielsetzung vgl. die Begründung zu § 30) in den Absätzen 1 bis 3. Diese sind entsprechenden gewerberechtl. Vorschriften weitgehend angeglichen. In Absatz 4 wird klargestellt, daß die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnittes unterliegenden Gewerbebetriebe unberührt bleibt.

Zum fünften Abschnitt –

Straf- und Bußgeldvorschriften

Zu § 32 – Straftaten

Durch diese Vorschriften soll der mit dem Gesetz beabsichtigte verstärkte Schutz der Privatsphäre dadurch gewährleistet werden, daß der Verstoß gegen die Bestimmungen in den Abschnitten 2 bis 4 über die Zulässigkeit der Veränderung und Weitergabe von personenbezogenen Daten sowie gegen andere einschlägige Vorschriften (vgl. § 37) unter Strafe gestellt wird. Sie knüpfen dabei an diese Regelungstatbestände an. Unbefugtes Handeln ist danach gegeben, wenn es gegen die entsprechenden Regelungen verstößt. Dabei werden auch die Fälle erfaßt, in denen nicht zum bei der Datenverarbeitung beschäftigten Personal gehörende Dritte personenbezogene Daten unbefugt verändern oder weitergeben.

In Absatz 1 wird die unbefugte Weitergabe, der Tatbestand, von dem die größte Gefahr für die Privatsphäre ausgehen kann, unter Strafe gestellt. Die Strafandrohung wird in Absatz 2 verschärft, wenn der Täter gegen Entgelt oder in Schädigungs- oder Bereicherungsabsicht handelt. Von diesen Voraussetzungen wird hier auch die Strafbarkeit des unbefugten Veränderns abhängig gemacht.

Es bleibt zu prüfen, ob diese Strafvorschriften wegen ihrer allgemeinen Bedeutung in das StGB aufgenommen werden sollen. In § 203 Abs. 2 Satz 1 StGB i.d.F. des Entwurfs eines Einführungsgesetzes zum StGB (BR-Drucksache 111/73) ist bislang nur der im vorstehenden § 32 Abs. 1 Nr. 1 aufgeführte Fall erfaßt.

Zu § 33 – Verletzung der Geheimhaltungspflicht

Da die Bediensteten der Aufsichtsbehörde in Ausübung ihrer Tätigkeit unter Umständen weitgehende Einblicke in betriebsinterne Angelegenheiten gewinnen können, sichert der Entwurf ihre Geheimhaltungspflicht strafrechtlich ab. Die bei den vom fünften Abschnitt erfaßten Stellen gespeicherten personenbezogenen Daten, die den Bediensteten im Laufe ihrer Tätigkeit bekannt werden, sind durch § 32 gegen Mißbräuche hinlänglich geschützt.

Zu § 34 – Ordnungswidrigkeiten

Die Vorschrift enthält Ordnungswidrigkeitstatbestände. Es handelt sich dabei um vorsätzliche oder fahrlässige Verstöße gegen Verfahrensvorschriften des Gesetzes, während durch die Strafbestimmungen in § 32 die Verletzung materieller Datenschutzbestimmungen geahndet werden. Auf diese Weise soll die korrekte Einhaltung der Verfahrensvorschriften, die eine wichtige Ergänzung der materiellen Regelungsvorschriften darstellen, gewährleistet werden.

Zum sechsten Abschnitt –

Übergangs- und Schlußvorschriften

Zu § 35 – Übergangsvorschriften

Die Vorschrift dient dazu, den Personen, Stellen usw., die bei Inkrafttreten des Gesetzes schon Datenverarbeitung betreiben, die Erfüllung bestimmter Verfahrensvorschriften zu erleichtern.

Zu § 36 – Anwendung des Verwaltungsverfahrensgesetzes

Durch diese Vorschrift wird das Verwaltungsverfahrensgesetz, das dem Parlament als Regierungsentwurf vorliegt, auch insoweit für anwendbar erklärt, als es von den Ländern ausgeführt wird. Sie folgt aus § 1 Abs. 2 Satz 2 des Entwurfs des Verwaltungsverfahrensgesetzes. Für die Durchführung des zweiten Abschnitts sowie der §§ 30 und 31 kann insbesondere die Anwendung der Vorschriften über die Amtshilfe (§§ 4 bis 7) und des Teils II – Allgemeine Vorschriften über das Verwaltungsverfahren – von Bedeutung sein.

Zu § 37 – Weitergeltende Datenschutzbestimmungen

Durch die Vorschrift wird der Grundsatz festgelegt, daß dem Datenschutz dienende bundesrechtliche

Spezialvorschriften, soweit sie auf in Dateien gespeicherte personenbezogene Daten anzuwenden sind, den Vorschriften dieses Gesetzes vorgehen. Dies wird verdeutlicht durch eine beispielhafte Aufzählung solcher Spezialvorschriften. Dieser Grundsatz wird in Satz 3 auf die in § 300 StGB genannten Berufsgeheimnisse erstreckt.

Zu § 38 – Berlin-Klausel

Die Vorschrift enthält die übliche Berlin-Klausel.

Zu § 39 – Inkrafttreten

Es ist vorgesehen, daß das Gesetz etwa ein Jahr nach der Verkündung in Kraft tritt, um es den vom Gesetz betroffenen datenverarbeitenden Personen, Behörden, Unternehmen und sonstigen Stellen zu ermöglichen, sich auf die sie neu treffenden Pflichten einzustellen. Davon abweichend treten die zum Erlaß von Rechtsverordnungen und allgemeinen Verwaltungsvorschriften ermächtigenden Vorschriften dieses Gesetzes am Tage nach der Verkündung in Kraft, um deren frühzeitige Vorbereitung zu ermöglichen.

Stellungnahme des Bundesrates

1. Zu § 2

a) In Absatz 1 sind

Satz 1 wie folgt zu fassen:

„Dieses Gesetz schützt personenbezogene Daten, soweit sie

1. von Behörden oder sonstigen öffentlichen Stellen (§ 5),
2. von natürlichen oder juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts für eigene Zwecke (§ 16),
3. von natürlichen oder juristischen Personen, Gesellschaften oder anderen Personenvereinigungen des privaten Rechts geschäftsmäßig für Dritte (§ 23)

in Dateien verarbeitet werden.“

und Satz 2 zu streichen.

Begründung

Der Gesetzentwurf erwähnt in anderen Vorschriften (vgl. § 2 Abs. 2, § 16 Abs. 1, § 23 Abs. 1) ausdrücklich natürliche und juristische Personen. Daher sollte § 2 Abs. 1 an diese Terminologie angepaßt werden.

Die Speicherung von Daten ist nach § 3 Abs. 2 Nr. 1 ein Unterfall der Datenverarbeitung und sollte deshalb in § 2 Abs. 1 nicht besonders erwähnt werden.

Der Datenschutz muß, um Beeinträchtigungen schutzwürdiger Belange der Bürger möglichst umfassend zu vermeiden, alle Dateien erfassen, unabhängig davon, ob die in ihnen enthaltenen Daten für die Weitergabe an Dritte bestimmt sind oder nicht. Die vorgesehene Einschränkung ist außerdem nicht praktikabel. Schließlich kann die Einschränkung dazu führen, daß Dateien nur deswegen unter das Gesetz fallen, weil sie in Rechenzentren, nicht aber in behördeneigenen Datenverarbeitungsanlagen gespeichert sind. Dadurch kann die Einrichtung einer rationellen Datenverarbeitungsorganisation behindert werden.

b) In Absatz 2 Satz 2 ist vor den Worten „zu publizistischen Zwecken“ das Wort „ausschließlich“ einzufügen.

Begründung

Durch die Einfügung des Wortes „ausschließlich“ soll die sonst bestehende Gefahr einer Umgehung datenschutzrechtlicher Vorschriften verringert werden.

- c) Der Bundesrat empfiehlt, im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen, ob die in § 2 Abs. 2 Satz 2 von der Anwendung des Gesetzes ausgenommenen Dateien den Vorschriften gegen einen mißbräuchlichen Abruf der gespeicherten Daten durch Unbefugte zu unterstellen sind.

2. Zu § 3

- a) Die Bundesregierung wird gebeten, im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen, ob die Begriffe „Speichernde Stelle“ und „Sperrern“ im Rahmen des § 3 näher konkretisiert werden können.

- b) In § 3 Abs. 2 wird der Terminus „Datenverarbeitung“ legal als das „Speichern, Verändern, Weitergeben oder Löschen von Daten“ definiert. Gleichwohl verwendet der Gesetzentwurf in einer Reihe von Bestimmungen (z. B. § 5 Abs. 3 Satz 1, § 13 Abs. 1, § 16 Abs. 1 und 2 und § 23 Nr. 3) die Ausdrücke „Speichern“ und „verarbeiten“ nebeneinander. Diese Tautologie ist nicht nur überflüssig, sondern führt in einigen Bestimmungen auch zu Unklarheiten und Divergenzen.

Die Bundesregierung wird daher gebeten, die entsprechenden Bestimmungen des Gesetzentwurfs im Hinblick auf die Legaldefinition in § 3 Abs. 2 zu überarbeiten.

3. Zu § 4

In Absatz 1 Satz 1 sind nach dem Zitat „§ 2 Abs. 1“ die Worte „oder im Auftrag der dort genannten Stellen oder Personen“ einzufügen.

Begründung

§ 4 Abs. 1 verwischt die auch von § 5 Abs. 3 Satz 2 anerkannte Trennung von zuständiger Behörde einerseits und Rechenzentrum andererseits, wenn das Rechenzentrum nur als reiner Dienstleistungsbetrieb eingesetzt wird. Denn die Rechtsverordnung nach § 4 Abs. 2 wendet sich an denjenigen, der nach § 4 Abs. 1 die

erforderlichen Maßnahmen zu treffen hat. Adressaten der Rechtsverordnung sind somit, da § 4 Abs. 1 lediglich auf § 2 Abs. 1 verweist, nur die in § 2 Abs. 1 genannten Stellen und somit nicht Rechenzentren, die nur im Auftrag der dort genannten Behörden tätig sind. Da sich aber Regelungen nach § 4 Abs. 2 in erster Linie an Rechenzentren richten sollen, zumal diese nach § 5 Abs. 3 Satz 2 von der Anwendung des 2. Abschnitts ausgeschlossen sind, ist hierfür in § 4 Abs. 1 eine Klarstellung erforderlich.

4. Zu § 5

a) Es sind

in Absatz 1 der Satz 2 zu streichen und nach Absatz 1 folgender Absatz 1 a einzufügen:

„(1 a) Die Vorschriften dieses Abschnitts gelten mit Ausnahme der §§ 14 und 15 auch für Behörden und sonstige Stellen der Länder, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen, soweit sie Bundesrecht ausführen oder soweit es sich um Gerichte oder Behörden der Staatsanwaltschaft handelt. Für die Ausführung von Bundesgesetzen, die nach Inkrafttreten dieses Gesetzes erlassen werden, gilt dies nur, soweit die Bundesgesetze die Vorschriften dieses Abschnitts für anwendbar erklären.“

Begründung

Artikel 84 Abs. 1 und Artikel 85 Abs. 1 GG gewähren dem Bund keine selbständige Gesetzgebungszuständigkeit für den Erlass von Verfahrensregelungen; sie setzen vielmehr eine Gesetzgebungskompetenz des Bundes voraus und ermöglichen nur, Verfahrensvorschriften als Annex-Kompetenz zu den in seinen Zuständigkeitsbereich fallenden Gesetzen zu treffen. Aus diesem Grund können Verfahrensregelungen nicht losgelöst von den materiellen Bestimmungen in einem Verwaltungsverfahrensgesetz des Bundes für die Verwaltungsbehörden geregelt werden. Diese Abhängigkeit der Verfahrensvorschriften von der ihnen zugrunde liegenden materiellen Norm schließt es aus, daß bereits Verfahrensregelungen für künftige bundesrechtliche Vorschriften in das Gesetz einbezogen werden.

b) In Absatz 3 ist Satz 1 wie folgt zu fassen:

„Die Vorschriften dieses Abschnitts gelten für die in Absatz 1 genannten Behörden und sonstigen Stellen auch insoweit, als die Verarbeitung personenbezogener Daten in Dateien in deren Auftrag durch andere Stellen betrieben wird.“

Begründung

Anpassung an die Begriffsbestimmung in § 3 Abs. 2 Nr. 1, nach der das Speichern einen Unterfall der Datenverarbeitung darstellt.

5. Zu § 7

a) In Absatz 1 ist Satz 2 wie folgt zu fassen:

„Die Weitergabe anderer personenbezogener Daten ist im Rahmen rechtmäßiger Erfüllung der in der Zuständigkeit der weitergebenden Stelle oder des Empfängers liegenden Aufgaben zulässig.“

Begründung

Die Vorschrift soll auch den sog. aktiven Datenaustausch erfassen und muß sich daher auch auf die Fälle erstrecken, in denen die Weitergabe, wie z. B. bei den Standesämtern, zur rechtmäßigen Aufgabenerfüllung der weitergebenden Stelle gehört.

b) Die Bundesregierung wird gebeten, im weiteren Verlauf des Gesetzgebungsverfahrens sicherzustellen, daß die Protokollierungspflicht nach § 7 Abs. 3 Satz 3 des Gesetzesentwurfs nicht eingreift, wenn Finanzbehörden im Rahmen ihrer Zuständigkeit personenbezogene Daten selbstständig abrufen, die von (anderen) Finanzbehörden oder in deren Auftrag gespeichert werden.

6. Zu §§ 7, 8 und 18

Der Bundesregierung wird empfohlen zu prüfen, ob die § 7 Abs. 1, § 8 Abs. 1 und § 18 so umgestellt werden können, daß die jeweils in Satz 2 enthaltene allgemeine Regelung vor die spezielle Regelung in Satz 1 gestellt wird.

7. Zu § 8

In Absatz 2 sind Nummern 3 und 4 zu streichen.

Begründung

Anpassung an § 19 Abs. 5 des Entwurfs eines Bundesmeldegesetzes.

8. Zu § 10

a) Satz 1 ist wie folgt zu fassen:

„Behörden oder sonstige öffentliche Stellen geben die Art der von ihnen oder in ihrem Auftrag gespeicherten personenbezogenen Daten, den betroffenen Personenkreis sowie die Stellen, an die sie personenbezogene Daten regelmäßig weitergeben, sowie die

Art der weiterzugebenden Daten unverzüglich nach der ersten Einspeicherung in dem für ihren Bereich bestehenden Veröffentlichungsblatt für amtliche Bekanntmachungen bekannt.“

Begründung

Durch die Änderung soll herausgestellt werden, daß die Behörde usw., die Daten verarbeiten läßt, und nicht das jeweilige Rechenzentrum für die Veröffentlichung verantwortlich ist. Die Bekanntgabe der Stellen, an die Daten weitergegeben werden, ist erforderlich, damit der Bürger seine Auskunfts- usw. -rechte auch gegenüber diesen Stellen wahrnehmen kann.

Die Veröffentlichung des Umfangs der gespeicherten Daten ist überflüssig, da rein numerische Angaben niemandem dienen. Die Veröffentlichung des Inhalts des Datensatzes muß ausreichen. Der letzte Halbsatz („... in Dateien speichern oder sonst verarbeiten“) ist im Hinblick auf § 3 überflüssig.

- b) Nach Satz 1 ist folgender Satz einzufügen:

„Die Landesregierungen werden ermächtigt, für die Behörden und sonstigen Stellen der Länder, der Gemeinden und Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und für deren Vereinigungen durch Rechtsverordnung das Veröffentlichungsblatt zu bestimmen.“

Begründung

Der Vorschlag ermöglicht es den Ländern, bei Bedarf eine zu starke Streuung der Veröffentlichungen zu verhindern.

- c) In Satz 2 sind die Worte „speichern oder sonst“ zu streichen.

Begründung

Anpassung an die Begriffsbestimmung in § 3 Abs. 2 Nr. 1. Danach ist es den Speichern ein Unterfall der Datenverarbeitung.

- d) Es ist folgender Satz anzufügen:

„Satz 1 gilt ferner nicht für gesetzlich vorgeschriebene Register oder sonstige auf Grund von Rechts- oder veröffentlichten Verwaltungsvorschriften zu führende Dateien, soweit die Art der in ihnen gespeicherten personenbezogenen Daten sowie der betroffene Personenkreis in Rechts- oder veröffentlichten Verwaltungsvorschriften festgelegt sind.“

Begründung

Für eine Vielzahl öffentlicher Register, die von Gerichten und Behörden geführt werden, sind Art und Umfang der zu speichernden Daten gesetzlich oder auf Grund von Rechts- oder veröffentlichten Verwaltungsvorschriften festgelegt. Das gilt z. B. sowohl für die Eintragung in die bei den Amtsgerichten zu führenden Vereins-, Handels-, Güterrechts- und Genossenschaftsregister sowie die Grundbücher als auch für die bei den Standesämtern zu führenden Personenstandsregister. Eine allgemeine Bekanntmachung nach Satz 1 könnte daher nur zur überflüssigen Wiederholung der bereits veröffentlichten Vorschriften führen.

9. Zu § 11

In Absatz 3 ist Nummer 2 wie folgt zu fassen:

„2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.“

Begründung

Verdeutlichung des Gewollten.

10. Zu §§ 11, 20 und 26

Im ärztlichen Bereich gibt es Erfahrungen, daß Patienten zwar eine rückhaltlose Aufklärung über alle sie betreffenden Fakten vom Arzt verlangen, der vollen Wahrheit jedoch nicht gewachsen sind und dann Kurzschlußhandlungen begehen. In solchen Fällen muß die Auskunft verweigert werden können.

Die Bundesregierung wird gebeten zu überprüfen, ob die Bestimmungen des Gesetzentwurfs allen Notwendigkeiten in diesem Bereich hinreichend Rechnung tragen.

11. Zu § 12

In Absatz 3 Satz 2 ist das Wort „geboten“ durch das Wort „unerlässlich“ zu ersetzen.

Begründung

Die Verwertung gesperrter Daten, die die speichernde Stelle nicht mehr zur rechtmäßigen Erfüllung ihrer Aufgaben benötigt, muß im Interesse des Persönlichkeitsschutzes auf das unerlässlich notwendige Maß beschränkt werden.

12. Zu § 13

In Absatz 1 sind im letzten Halbsatz die Worte „gespeichert und sonst“ zu streichen.

Begründung

Anpassung an die Begriffsbestimmung in § 3 Abs. 2 Nr. 1, wonach das Speichern ein Unterfall der Datenverarbeitung ist.

13. Zu § 15

In § 15 sind nach den Worten „Bundesbahn erlassen“ die Worte „im Einvernehmen mit dem Bundesminister des Innern“ einzufügen.

Begründung

Der Bundesminister des Innern soll beteiligt werden, um den Erlaß einheitlicher Vorschriften sicherzustellen. Die Einheitlichkeit ist erforderlich, da davon ausgegangen werden muß, daß in den Rechenzentren Aufgaben aus verschiedenen Geschäftsbereichen abgewickelt werden. Es wäre unerträglich, wenn in den einzelnen Rechenzentren voneinander abweichende, generelle Regelungen beachtet werden müßten.

14. Zu § 16

Es sind

in Absatz 1 Satz 1 im zweiten Halbsatz die Worte „speichern und sonst“ zu streichen und in Absatz 2 der zweite Halbsatz wie folgt zu fassen:

„als die Verarbeitung personenbezogener Daten in Dateien in deren Auftrag durch andere Stellen betrieben wird.“

Begründung

Anpassung an die Begriffsbestimmung in § 3 Abs. 2 Nr. 1, wonach das Speichern ein Unterfall der Datenverarbeitung ist.

15. Zu § 20

In Absatz 3 ist Satz 2 wie folgt zu fassen:

„Ein Entgelt kann in den Fällen nicht verlangt werden, in denen durch besondere Umstände die Annahme gerechtfertigt wird, daß personenbezogene Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergeben hat, daß die personenbezogenen Daten zu berichtigen oder unter der Voraussetzung des § 21 Abs. 2 Satz 2 zu löschen sind.“

Begründung

Die Regelung des § 20 Abs. 3 Satz 2 weicht ohne ersichtlichen Grund von der Regelung des § 11 Abs. 4 ab. Nach § 11 Abs. 4 hat der einzelne die Möglichkeit, gegenüber Behörden geltend zu machen, daß besondere Umstände die Annahme rechtfertigen, daß personenbezogene

Daten unrichtig oder unzulässig gespeichert werden. Er muß, wenn diese Umstände vorliegen, eine gebührenfreie Auskunft erhalten, auch wenn die Auskunft ergibt, daß eine Berichtigung oder Löschung nicht notwendig ist.

Der Bürger kann also, wenn die genannten Umstände gegeben sind, die Datenspeicherung überprüfen, ohne im Falle seines Irrtums eine Gebühr bezahlen zu müssen.

Im Gegensatz dazu sieht § 20 Abs. 3 im Falle der privaten Datenverarbeitung eine Erteilung der Auskunft Zug um Zug gegen Bezahlung des Entgelts vor.

Die Überprüfung, ob eine Berichtigung notwendig ist, kann der Betroffene aber erst nach der Bezahlung beginnen – auch dann, wenn auf Grund besonderer Umstände die Annahme gerechtfertigt war, daß Daten unrichtig oder unzulässig gespeichert werden. Er wird damit in jedem Fall in die Rolle dessen gedrängt, der sein Entgelt zurückfordern muß.

Diese Schlechterstellung des Bürgers leuchtet nicht ein; insbesondere da Behörden in ihrer Tätigkeit ohnehin alle Rechtsstaatsgarantien gegenüber dem Bürger einzuhalten haben, während sich Private lediglich im Rahmen des Zivil- und Strafrechts halten müssen.

Es wird daher für richtig gehalten, eine Auskunft ohne Entgelt in all den Fällen privater Datenverarbeitung vorzusehen, in denen entsprechend der Regelung von § 11 Abs. 4 besondere Umstände die Annahme rechtfertigen, daß personenbezogene Daten unrichtig oder unzulässig gespeichert werden.

16. Zu § 23

a) Es sind in Nummer 1 im zweiten Halbsatz die Worte „verändert oder sonst“ und in Nummer 3 im ersten Halbsatz die Worte „speichern oder sonst“ zu streichen.

Begründung

Anpassung an die Begriffsbestimmung in § 3 Abs. 2 Nr. 1. Danach sind sowohl das Verändern als auch das Speichern Unterfälle der Datenverarbeitung.

b) In Nummer 3 sind die Worte „zum Zweck der Datenverarbeitung“ durch die Worte „als Dienstleistungsunternehmen“ zu ersetzen.

Begründung

Die Formulierung „Daten zum Zweck der Datenverarbeitung verarbeiten“ läßt nicht erkennen, daß es hierbei lediglich um die Erbringung von Dienstleistungsfunktionen geht. Dies sollte durch eine klare Formulierung ausgedrückt werden.

17. Zu § 24

Absatz 3 ist wie folgt zu fassen:

„(3) Abweichend von Absatz 2 Satz 1 ist die Weitergabe zulässig, wenn sie sich auf freie Daten (§ 8 Abs. 2) beschränkt.“

Begründung

Die Regelung des § 24 Abs. 3 ist in ihrer zweiten Alternative ohne Einschränkung oder wenigstens Bezeichnung der weiteren persönlichen Merkmale nicht tragbar, da sie der Gefahr künftigen Mißbrauchs nicht die geringste Schranke setzt. Denn § 24 Abs. 3 eröffnet in seiner zweiten Alternative die Möglichkeit, über mehrfache Weitergaben und anschließende Verknüpfung der empfangenen Daten durch den Empfänger sich alle von Privaten über eine bestimmte Person gespeicherten Daten zu verschaffen.

18. Zu § 26

In Absatz 3 ist Satz 2 wie folgt zu fassen:

„Ein Entgelt kann in den Fällen nicht verlangt werden, in denen durch besondere Umstände die Annahme gerechtfertigt wird, daß personenbezogene Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergeben hat, daß die personenbezogenen Daten zu berichtigen oder unter der Voraussetzung des § 27 Abs. 3 Satz 2 zu löschen sind.“

Begründung

Folge des Änderungsvorschlags zu § 20 Abs. 3 Satz 2.

19. Zu § 30

In Absatz 2 ist folgende Nummer 7 anzufügen:

„7. bei regelmäßiger Weitergabe personenbezogener Daten Empfänger und Art der weitergegebenen Daten.“

Begründung

Folge des Änderungsvorschlags zu § 10 Satz 1.

20. Zu § 31

In § 31 wird folgender Absatz 5 angefügt:

„(5) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Überwachung der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnitts zuständigen Aufsichtsbehörden.“

Begründung

Die Vorschrift soll die Bestimmung der zuständigen Aufsichtsbehörde durch Rechtsverordnung ermöglichen, soweit nach Landesverfassungsrecht für die Bestimmung der zuständigen Behörde ein Rechtssatz erforderlich ist und in den Ländern eine landesrechtliche Ermächtigung zum Erlaß von Organisationsrechtsverordnungen fehlt.

21. Zu § 34

- a) In Absatz 1 sind in Nummer 1 hinter „§ 16 Abs. 1“ die Worte „oder 2“ einzufügen.

Begründung

Notwendige Berichtigung.

- b) In Absatz 1 ist in Nummer 4 und 5 jeweils das Wort „und“ durch das Wort „oder“ zu ersetzen.

Begründung

Notwendige Klarstellung.

22. Zu § 37

Es sind

- a) in Satz 1 die Worte „dem Datenschutz dienende“ zu streichen;

- b) Nummer 3 wie folgt zu fassen:

„3. Vorschriften über die Verpflichtung, die Beschränkung oder das Verbot der Weitergabe oder Veröffentlichung von Einzelangaben über Personen, z. B. § 161 der Strafprozeßordnung, § 7 Abs. 4, ... (weiter wie Entwurf).“ und

- c) die Überschrift wie folgt zu fassen:

„Weitergeltende Vorschriften“.

Begründung

Zu a)

Klarstellung, daß auch besondere Rechtsvorschriften des Bundes, die Geheimhaltungs- und Auskunftspflichten betreffen, vorgehen.

Zu b)

Notwendige Ergänzung.

Zu c)

Folge des Änderungsvorschlags zu a).

23. Zum Gesetzentwurf im ganzen

- a) Die Bundesregierung wird gebeten, im weiteren Verlauf des Gesetzgebungsverfahrens Definitionen und Formulierungen im Entwurf eines Bundesmeldegesetzes und im Entwurf eines Bundes-Datenschutzgesetzes zu harmonisieren.

- b) Die Bundesregierung wird gebeten, den Entwurf eines Gesetzes zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundes-Datenschutzgesetz – BDSG) mit dem Entwurf eines Verwaltungsverfahrensgesetzes abzustimmen. Regelungen des Verwaltungsverfahrens sollten grundsätzlich im Verwaltungsverfahrensgesetz getroffen werden. Abweichende Regelungen im Entwurf des Bundes-Datenschutzgesetzes sollten nur da vorgesehen werden, wo sie wegen der Besonderheit der Materie geboten erscheinen. Nach dieser Überlegung sollten insbesondere die §§ 7, 8 und 11 des Entwurfs eines Bundes-Datenschutzgesetzes auf ihre Vereinbarkeit mit den §§ 4 bis 8, 21 und 25 des Entwurfs eines Verwaltungsverfahrensgesetzes – BR-Drucksache 227/73 (Beschluß) – überprüft werden.

Gegenäußerung der Bundesregierung zu der Stellungnahme des Bundesrates

Zu 1. a) (§ 2 Abs. 1)

- a) Die Bundesregierung erhebt gegen die in der vorgeschlagenen Neufassung des Satzes 1 enthaltene terminologische Anpassung an entsprechende Regelungen in § 16 Abs. 1 und § 23 Abs. 1 des Entwurfs (natürliche und juristische Personen werden dort ausdrücklich erwähnt) keine Einwendungen.
- b) Der mit der Neufassung des Satzes 1 verbundene Streichung der Worte „gespeichert und sonst“ stimmt die Bundesregierung nicht zu. Nicht alle in § 3 Abs. 2 definierten Phasen der Datenverarbeitung erfolgen zwangsläufig ausschließlich in Dateien. Es wird sich z. B. das Bekanntgeben der durch die Datenverarbeitung unmittelbar gewonnenen Daten vielmehr in der Regel außerhalb einer Datei abspielen. Um auch diesen Vorgang zu erfassen, ist hier die Formulierung „in Dateien gespeichert und sonst verarbeitet“ für erforderlich gehalten worden. Durch die vom Bundesrat vorgeschlagene Änderung würde also eine – von ihm wohl nicht gewollte – Verengung des Anwendungsbereiches des Gesetzes erreicht werden. Es wird jedoch im weiteren Gesetzgebungsverfahren zu prüfen sein, ob nicht durch die Formulierung „in Dateien gespeichert und innerhalb oder außerhalb von Dateien in anderer Weise verarbeitet werden“ das Gewollte klarer zum Ausdruck gebracht werden kann.
- c) Der Streichung des mit den Worten „es sei denn ...“ beginnenden letzten Halbsatzes von Satz 1 und des Satzes 2 kann nicht zugestimmt werden, weil in der Regel Gefährdungen der Privatsphäre nicht schon mit der Speicherung personenbezogener Daten, sondern erst mit deren Weitergabe an Dritte einsetzen und daher Daten, die zum ausschließlich internen Gebrauch bestimmt sind, auch aus Gründen der leichteren Handhabbarkeit nicht unter das Gesetz zu fallen brauchen. Satz 2 stellt dabei sicher, daß Daten, die im Einzelfall entgegen der ursprünglichen Zweckbestimmung doch an Dritte weitergegeben werden, uneingeschränkt durch das Gesetz geschützt werden.

Zu 1. b) (§ 2 Abs. 2 Satz 2)

Dem Vorschlag des Bundesrates wird zugestimmt.

Zu 1. c) (§ 2 Abs. 2 Satz 2)

Die Bundesregierung wird diese Frage im weiteren Verlauf des Gesetzgebungsverfahrens prüfen.

Zu 2. a) (§ 3)

Die Bundesregierung wird diese Frage im weiteren Verlauf des Gesetzgebungsverfahrens prüfen.

Zu 2. b) (§ 3 Abs. 2)

Die Bundesregierung wird den Vorschlag des Bundesrates nach Maßgabe ihrer Ausführungen zu 1. a) (unter Buchstabe b bzw. zu den entsprechenden Punkten der Stellungnahme des Bundesrates [vgl. 4. b), 8. c), 12., 14., 16. a)]) im weiteren Gesetzgebungsverfahren prüfen.

Zu 3. (§ 4 Abs. 1 Satz 1)

Gegen den Vorschlag des Bundesrates werden keine Einwendungen erhoben.

Zu 4. a) (§ 5 Abs. 1)

Die Bundesregierung stimmt dem Vorschlag des Bundesrates nicht zu. Sie ist der Auffassung, daß aus der Akzessorietät der Verfahrensregelung zur Sachregelung nicht gefolgert werden kann, der Bund könne Verfahrensregelungen zu Bundesgesetzen, die nach den Artikeln 84 und 85 GG durch die Länder ausgeführt werden, nur treffen, wenn diese Gesetze bereits ergangen sind oder zugleich mit der Verfahrensregelung ergehen, nicht aber, wenn sie erst künftig ergehen sollen. Die Auffassung des Bundesrates, wonach sich eine solche dem Gebot möglichst rationeller und systematischer Gesetzgebung zuwiderlaufende Beschränkung aus dem Wesen der Annex-Kompetenz ergäbe, trifft nicht zu. Da der Bund in allen nach den Artikeln 84 und 85 GG zu vollziehenden Bundesgesetzen gleichlautende Verfahrensregeln treffen kann, muß es auch zulässig sein, das gleiche Ziel mit einer einheitlichen Verfahrensregelung zu erreichen, die auch für künftig zu erlassende Sachregelungen des Bundes gilt.

Zu 4. b) (§ 5 Abs. 3 Satz 1)

Die Bundesregierung stimmt dem Vorschlag des Bundesrates aus den zu 1. a) unter Buchstabe b genannten Gründen nicht zu. Es wird jedoch im weiteren Gesetzgebungsverfahren zu prüfen sein, ob nicht im Rahmen der Regelung dieser Vorschrift die Worte „das Speichern in Dateien und“ sowie „sonstige“ entbehrlich sind und durch ihre Streichung das Gewollte klarer zum Ausdruck gebracht werden kann.

Zu 5. a) (§ 7 Abs. 1 Satz 2)

Gegen den Vorschlag des Bundesrates werden keine Einwendungen erhoben.

Zu 5. b) (§ 7 Abs. 3 Satz 3)

Die Bundesregierung wird diese seit geraumer Zeit in Diskussion befindliche Frage auch im weiteren Verlauf des Gesetzgebungsverfahrens prüfen.

Zu 6. (§ 7 Abs. 1, § 8 Abs. 1, § 18)

Der Vorschlag wird im weiteren Gesetzgebungsverfahren geprüft werden.

Zu 7. (§ 8 Abs. 2 Nr. 3 und 4)

Die Bundesregierung stimmt dem Vorschlag des Bundesrates nicht zu. Geburtsdatum und Berufs- bzw. Branchen- oder Geschäftsbezeichnung sind im allgemeinen ohnehin offenkundig und bedürfen keines besonderen Schutzes. Ihre Aufnahme unter die „freien Daten“ dient der leichteren Handhabung des Gesetzes. Dies ist sowohl für die Verwaltung als auch für den betroffenen Bürger von Bedeutung (vgl. z. B. die Notwendigkeit der fristgerechten Neuherausgabe der Amtlichen Fernsprechbücher und der Branchen-Fernsprechbücher sowie der fernmündlichen Auskunftserteilung im Fernsprechdienst). Mit Rücksicht auf grundlegende Unterschiede hinsichtlich Anwendungsbereich und Zielsetzung des Bundes-Datenschutzgesetzes bedarf es einer Angleichung an den Entwurf des Bundesmeldegesetzes insoweit nicht. Auf die Ausführungen der Bundesregierung zu Punkt 23 a) der Stellungnahme des Bundesrates wird in diesem Zusammenhang Bezug genommen.

Zu 8. a) (§ 10 Satz 1)

Gegen den Vorschlag des Bundesrates werden keine Einwendungen erhoben.

Zu 8. b) (§ 10 Satz 1 a)

Die Bundesregierung wird den Vorschlag des Bundesrates im weiteren Verlauf des Gesetzgebungsverfahrens prüfen; sie behält sich vor, auch für sich eine entsprechende Ermächtigung vorzuschlagen.

Zu 8. c) (§ 10 Satz 2)

Die Bundesregierung stimmt dem Vorschlag des Bundesrates aus den zu 1. a) unter Buchstabe b genannten Gründen nicht zu. Es wird jedoch im weiteren Gesetzgebungsverfahren zu prüfen sein, ob nicht im Rahmen der Regelung dieser Vorschrift die Worte „oder sonst verarbeiten“ entbehrlich sind und durch ihre Streichung das Gewollte klarer zum Ausdruck gebracht werden kann.

Zu 8. d) (§ 10 Satz 2 a)

Dem Vorschlag des Bundesrates kann mit Rücksicht auf sein Petitum zu § 10 Satz 1 [Nr. 8 a) der Stellungnahme] nur mit der Maßgabe zugestimmt werden, daß die in dem neu anzufügenden Satz vorge-

sehenen Ausnahmen von der Veröffentlichungspflicht nur dann Platz greifen, soweit in den Rechts- oder veröffentlichten Verwaltungsvorschriften auch die Stellen, an die personenbezogene Daten regelmäßig weitergegeben werden, sowie die Art der weiterzugebenden Daten festgelegt sind.

Zu 9. (§ 11 Abs. 3 Nr. 2)

Dem Vorschlag des Bundesrates wird zugestimmt.

Zu 10. (§§ 11, 20 und 26)

Die Bundesregierung hat dem Problemkomplex der ärztlichen Aufklärungspflicht vom Beginn der Vorbereitung dieses Gesetzentwurfs an ihre Aufmerksamkeit gewidmet. Sie ist der Auffassung, daß die einschlägigen Bestimmungen des Entwurfs sich in Einklang mit der höchstrichterlichen Rechtsprechung sowie dem ärztlichen Standesrecht befinden. Das schließt nicht aus, daß diesem Fragenkreis auch im weiteren Verlauf des Gesetzgebungsverfahrens besondere Beachtung zugewendet wird.

Zu 11. (§ 12 Abs. 3 Satz 2)

Dem Vorschlag des Bundesrates wird zugestimmt.

Zu 12. (§ 13 Abs. 1)

Die Bundesregierung stimmt dem Vorschlag des Bundesrates aus den zu 1. a) unter Buchstabe b genannten Gründen nicht zu. Es wird jedoch im weiteren Gesetzgebungsverfahren zu prüfen sein, ob nicht im Rahmen der Regelung dieser Vorschrift die Worte „in Dateien gespeichert und sonst“ entbehrlich sind und durch ihre Streichung das Gewollte klarer zum Ausdruck gebracht werden kann.

Zu 13. (§ 15)

Dem Vorschlag des Bundesrates wird nicht zugestimmt. Soweit ein Bedürfnis zur Regelung allgemeiner Grundsätze besteht, kann die Bundesregierung nach § 4 des Gesetzes eine Rechtsverordnung erlassen. Darüber hinaus gibt Artikel 86 GG ihr das Recht zum Erlaß allgemeiner Verwaltungsvorschriften. Ein Bedürfnis, auch noch die auf die Besonderheiten eines Geschäftsbereichs abgestellten Vorschriften einheitlich zu regeln, besteht daneben nicht.

Zu 14. (§ 16 Abs. 1 Satz 1, Abs. 2)

Die Bundesregierung stimmt den Vorschlägen des Bundesrates aus den zu 1. a) unter Buchstabe b genannten Gründen nicht zu. Es wird jedoch im weiteren Gesetzgebungsverfahren zu prüfen sein, ob nicht im Rahmen der Regelung dieser Vorschrift die Worte „in Dateien speichern und sonst“ in Absatz 1 sowie „das Speichern in Dateien und“ und „sonstige“ in Absatz 2 entbehrlich sind und durch ihre Streichung das Gewollte klarer zum Ausdruck gebracht werden kann.

Zu 15. (§ 20 Abs. 3 Satz 2)

Dem Vorschlag des Bundesrates wird zugestimmt.

Zu 16. a) (§ 23 Nr. 1 und 3)

Die Bundesregierung stimmt den Vorschlägen des Bundesrates aus den zu 1. a) unter Buchstabe **b** genannten Gründen nicht zu. Im übrigen kommt es in § 23 Nr. 1 gerade auf das Verändern an, weshalb diese Phase der Datenverarbeitung hier hervorgehoben wird. Es wird jedoch im weiteren Gesetzgebungsverfahren zu prüfen sein, ob nicht im Rahmen der Regelung dieser Vorschrift die Worte „oder sonst verarbeitet“ in Nummer 1 sowie „in Dateien speichern und sonst“ in Nummer 3 entbehrlich sind und durch ihre Streichung das Gewollte klarer zum Ausdruck gebracht werden kann.

Zu 16. b) (§ 23 Nr. 3)

Die Bundesregierung erhebt gegen den Vorschlag des Bundesrates keine Einwendungen.

Zu 17. (§ 24 Abs. 3)

Die Bundesregierung stimmt dem Vorschlag des Bundesrates nicht zu. Durch § 24 Abs. 3 des Regierungsentwurfs wird den Bedürfnissen der Werbewirtschaft auf eine mit dem Datenschutzgedanken durchaus verträgliche Weise Rechnung getragen. Neben „freien Daten“ darf die Datenweitergabe nur noch eine Angabe umfassen, die sich jedoch auf die Zugehörigkeit des Betroffenen zu einer Personengruppe beziehen muß. Künftigen Mißbräuchen ist eine weitere Schranke dadurch gesetzt, daß diese Datenweitergabe nicht geeignet sein darf, schutzwürdige Belange des Betroffenen zu beeinträchtigen.

Zu 18. (§ 26 Abs. 3 Satz 2)

Dem Vorschlag des Bundesrates wird zugestimmt.

Zu 19. (§ 30 Abs. 2 Nr. 7)

Dem Vorschlag des Bundesrates wird zugestimmt.

Zu 20. (§ 31 Abs. 5)

Dem Vorschlag des Bundesrates wird zugestimmt.

Zu 21. a) und b) (§ 34 Abs. 1 Nr. 1, 4 und 5)

Den Vorschlägen des Bundesrates wird zugestimmt.

Zu 22. (§ 37)

Dem Vorschlag des Bundesrates wird zugestimmt.

Zu 23. a) (Geszentwurf im ganzen)

Die Bundesregierung wird auch weiterhin, wie schon bisher, auf die Harmonisierung von Definitionen und Formulierungen im Entwurf eines Bundes-Datenschutzgesetzes und im Entwurf eines Bundesmeldegesetzes achten. Es hat sich jedoch ergeben, daß eine Reihe von Begriffen in den beiden Geszentwürfen wegen ihrer grundlegenden Unterschiede hinsichtlich Anwendungsbereich und Zielsetzung nicht vereinheitlicht werden können.

Zu 23. b) (Geszentwurf im ganzen)

Die Bundesregierung wird auch im weiteren Verlauf des Gesetzgebungsverfahrens auf eine Abstimmung des Entwurfs eines Bundes-Datenschutzgesetzes mit dem Entwurf eines Verwaltungsverfahrensgesetzes Wert legen. Abweichende Regelungen sind im Entwurf eines Bundes-Datenschutzgesetzes jedoch dort nicht zu vermeiden, wo sie wegen der erheblichen Besonderheiten dieser Materie zwingend geboten sind.