

01.06.90
In - R

Gesetzesbeschuß
des Deutschen Bundestages

Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes

Der Deutsche Bundestag hat in seiner 214. Sitzung am 31. Mai 1990 aufgrund der Beschlussempfehlung und des Berichts des Innenausschusses (4. Ausschuß) - Drucksache 11/7235 - den von der Bundesregierung eingebrachten

Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes

- Drucksache 11/4306 -

in der nachstehenden Fassung angenommen:

Fristablauf: 22.06.90

Erster Durchgang: Drs. 618/88

Alleinvertrieb: Verlag Dr. Hans Hegner, Postfach 20 08 21, 5300 Bonn 2
ISSN 0720-2846

Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes

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

Artikel 1

Bundesdatenschutzgesetz (BDSG)

Inhaltsübersicht

Erster Abschnitt: Allgemeine Bestimmungen	§§
Zweck und Anwendungsbereich des Gesetzes	1
Öffentliche und nicht-öffentliche Stellen	2
Weitere Begriffsbestimmungen	3
Zulässigkeit der Datenverarbeitung und -nutzung	4
Datengeheimnis	5
Unabhängige Rechte des Betroffenen	6
Schadensersatz durch öffentliche Stellen	7
Schadensersatz durch nicht-öffentliche Stellen	8
Technische und organisatorische Maßnahmen	9
Einrichtung automatisierter Abzufverfahren	10
Verarbeitung personenbezogener Daten im Auftrag	11
Zweiter Abschnitt: Datenverarbeitung der öffentlichen Stellen	
Erster Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung	
Anwendungsbereich	12
Datenerhebung	13
Datenspeicherung, -veränderung und -nutzung	14
Datenübermittlung an öffentliche Stellen	15
Datenübermittlung an nicht-öffentliche Stellen	16
Datenübermittlung an Stellen außerhalb des Geltungsbereichs dieses Gesetzes	17
Durchführung des Datenschutzes in der Bundesverwaltung	18
Zweiter Unterabschnitt: Rechte des Betroffenen	
Auskunft an den Betroffenen	19
Berichtigung, Löschung und Sperrung von Daten	20
Anrufung des Bundesbeauftragten für den Datenschutz	21

Dritter Unterabschnitt: Bundesbeauftragter für den Datenschutz	
Wahl	22
Rechtsstellung	23
Kontrolle durch den Bundesbeauftragten	24
Beauftragungen durch den Bundesbeauftragten	25
Weitere Aufgaben des Bundesbeauftragten, Datenregister	26
Dritter Abschnitt: Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen	
Erster Unterabschnitt: Rechtsgrundlagen der Datenverarbeitung	
Anwendungsbereich	27
Datenspeicherung, -übermittlung und -nutzung für eigene Zwecke	28
Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung	29
Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung in anonymisierter Form	30
Besondere Zweckbindung	31
Meldepflichten	32
Zweiter Unterabschnitt: Rechte des Betroffenen	
Benachrichtigung des Betroffenen	33
Auskunft an den Betroffenen	34
Berichtigung, Löschung und Sperrung von Daten	35
Dritter Unterabschnitt: Beauftragter für den Datenschutz, Aufsichtsbehörde	
Bestellung eines Beauftragten	36

379/90

	§§
Aufgaben des Beauftragten	37
Aufsichtsbehörde	38

Vierter Abschnitt: Sondervorschriften

Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsge- heimnis unterliegen	39
Verarbeitung und Nutzung personenbezoge- ner Daten für die wissenschaftliche For- schung	40
Verarbeitung und Nutzung personenbezoge- ner Daten durch die Medien	41
Datenschutzbeauftragte der Rundfunkanstal- ten des Bundesrechts	42

Fünfter Abschnitt: Schlußvorschriften

Strafvorschriften	43
Bußgeldvorschriften	44
Berlin-Klausel	45
Anlage zu § 9 Satz 1	

ERSTER ABSCHNITT

Allgemeine Bestimmungen

§ 1

Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
 - a) Bundesrecht ausführen oder
 - b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Dieses Gesetz gilt ferner für die Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen.

(4) Bei der Anwendung dieses Gesetzes gelten folgende Einschränkungen:

1. Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten nur die §§ 5 und 9.
2. Für nicht-automatisierte Dateien, deren personenbezogene Daten nicht zur Übermittlung an Dritte bestimmt sind, gelten nur die §§ 5, 9, 39 und 40. Außerdem gelten für Dateien öffentlicher Stellen die §§ 14 und 18 Abs. 1. Werden im Einzelfall personenbezogene Daten übermittelt, gelten für diesen Einzelfall die Vorschriften dieses Gesetzes uneingeschränkt.

(5) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

§ 2

Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie derer Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder
2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§ 3

Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Eine Datei ist

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei) oder
2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, ungeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, daß sie durch automatisierte Verfahren ungeordnet und ausgewertet werden können.

(3) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(4) Erheben ist das Beschaffen von Daten über den Betroffenen.

(5) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger) in der Weise, daß
 - a) die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder
 - b) der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(6) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(7) Anonymisieren ist das Verändern personenbezogener Daten derart, daß die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbar natürlichen Person zugeordnet werden können.

(8) Speichernde Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern läßt.

(9) Dritter ist jede Person oder Stelle außerhalb der speichernden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieses Gesetzes personenbezogene Daten im Auftrag verarbeiten oder nutzen.

§ 4

Zulässigkeit der Datenverarbeitung und -nutzung

(1) Die Verarbeitung personenbezogener Daten und deren Nutzung sind nur zulässig, wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder soweit der Betroffene eingewilligt hat.

(2) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

(3) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 2 Satz 2 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 2 Satz 1 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszweckes ergibt, schriftlich festzuhalten.

§ 5

Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 6

Unabdingbare Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen in einer Datei gespeichert, bei der mehrere Stellen speicherungsbe-rechtigt sind, und ist der Betroffene nicht in der Lage, die speichernde Stelle festzustellen, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die speichernde Stelle weiterzuleiten. Der Betroffene ist über die Weiterlei-tung und die speichernde Stelle zu unterrichten. Die

in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz unter-richten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

§ 7

Schadensersatz durch öffentliche Stellen

(1) Fügt eine öffentliche Stelle dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Daten-schutz unzulässige oder unrichtige automatisierte Verarbeitung seiner personenbezogenen Daten ei-nen Schaden zu, ist sie dem Betroffenen unabhängig von einem Verschulden zum Ersatz des daraus ent-stehenden Schadens verpflichtet.

(2) Bei einer schweren Verletzung des Persönlich-keitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu erset-zen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt bis zu einem Betrag von zweihundertfünf-zigtausend Deutsche Mark begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Scha-densersatz zu leisten, der insgesamt den Höchstbe-trag von zweihundertfünfzigtausend Deutsche Mark übersteigt, so verringern sich die einzelnen Scha-densersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer Datei mehrere Stellen speiche-rungsbe-rechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Mehrere Ersatzpflichtige haften als Gesamt-schuldner.

(6) Auf das Mitverschulden des Betroffenen und die Verjährung sind §§ 254 und 852 des Bürgerlichen Ge-setzbuches entsprechend anzuwenden.

(7) Vorschriften, nach denen ein Ersatzpflichtiger in weiterem Umfang als nach dieser Vorschrift haftet oder nach denen ein anderer für den Schaden verant-wortlich ist, bleiben unberührt.

(8) Der Rechtsweg vor den ordentlichen Gerichten steht offen.

§ 8

Schadensersatz durch nicht-öffentliche Stellen

Macht ein Betroffener gegenüber einer nicht-öf-fentlichen Stelle einen Anspruch auf Schadensersatz wegen einer nach diesem Gesetz oder anderen Vor-schriften über den Datenschutz unzulässigen oder unrichtigen automatisierten Datenverarbeitung gel-tend und ist streitig, ob der Schaden die Folge eines von der speichernden Stelle zu vertretenden Umstan-des ist, so trifft die Beweislast die speichernde Stelle.

§ 9

Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbei-ten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbe-sondere die in der Anlage zu diesem Gesetz genann-ten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 10

Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfah-rens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdi-gen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen ange-messen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, daß die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzule-gen:

1. Anlaß und Zweck des Abrufverfahrens,
2. Datenempfänger,
3. Art der zu übermittelnden Daten,
4. nach § 9 erforderliche technische und organisatori-sche Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Daten-schutz unter Mitteilung der Festlegungen nach Ab-satz 2 zu unterrichten. Die Einrichtung von Abrufver-

fahren, bei denen die in § 6 Abs. 1 und § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn die für die speichernde und die abrufende Stelle jeweils zuständigen Bundes- oder Landesminister oder deren Vertreter zugestimmt haben.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlaß besteht. Die speichernde Stelle hat zu gewährleisten, daß die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus Datenbeständen, die jedermann, sei es ohne oder nach besonderer Zulassung, zur Benutzung offenstehen.

§ 11

Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in § 6 und 7 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei die Datenverarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten oder nutzen. Ist er der Ansicht, daß eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 7, 13 Abs. 1, Abs. 3 und 4 sowie § 14 Abs. 1 Nr. 2, 5, 6 und 7 und Abs. 2 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,
- b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,

die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig verarbeiten oder nutzen die §§ 32, 36 bis 38.

ZWEITER ABSCHNITT

Datenverarbeitung der öffentlichen Stellen

ERSTER UNTERABSCHNITT

Rechtsgrundlagen der Datenverarbeitung

§ 12

Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§ 12 bis 13, 18 und 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder
2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Für Landesbeauftragte für den Datenschutz gilt § 23 Abs. 4 entsprechend.

(3) Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse verarbeitet oder genutzt, gelten anstelle der §§ 14 bis 17, 19 und 20 der § 28 Abs. 1 und 2 sowie die §§ 33 bis 35.

Nr. 1 und 2

§ 13

Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stellen erforderlich ist.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
- b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde

und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck ihm gegenüber anzugeben. Werden sie beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Auf Verlangen ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

(4) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§ 14

Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat,
3. offensichtlich ist, daß es im Interesse des Betroffenen liegt und kein Grund zu der Annahme besteht, daß er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
4. die Daten für den anderen Zweck aufgrund einer durch Rechtsvorschrift festgelegten Auskunftspflicht beim Betroffenen erhoben werden dürfen,
5. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
6. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Zweckänderung offensichtlich überwiegt,
7. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,

8. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuches oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist oder

9. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,

10. es zur Durchführung wissenschaftlicher Forschung erforderlich ist und das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt. Dies gilt nicht, wenn der Zweck der Forschung durch die Verwendung anonymisierter Daten erreicht werden kann.

In den Fällen der Nummer 4 unterrichtet die speichernde Stelle den Betroffenen über die Zweckänderung. Dies gilt nicht, wenn damit zu rechnen ist, daß er davon auf andere Weise Kenntnis erlangt.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die speichernde Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die speichernde Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§ 15

Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist und
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Empfängers, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt,

es sei denn, daß besonderer Anlaß zur Prüfung der Zulässigkeit der Übermittlung besteht. § 14 Abs. 4 bleibt unberührt.

(3) Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, daß bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, daß eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechnete Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

§ 16

Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder
2. der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, daß er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Empfänger darf die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 17

Datenübermittlung an Stellen außerhalb des Geltungsbereiches dieses Gesetzes

(1) Für die Übermittlung personenbezogener Daten an Stellen außerhalb des Geltungsbereiches dieses Gesetzes sowie an über- und zwischenstaatliche Stellen gilt § 14 Abs. 1 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, sowie § 14 Abs. 3.

(2) Eine Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde.

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(4) Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie ihm übermittelt werden.

§ 18

Durchführung des Datenschutzes in der Bundesverwaltung

(1) Die obersten Bundesbehörden, der Vorstand der Deutschen Bundesbahn, die Vorstände der Unternehmen der Deutschen Bundespost oder das Direktorium der Deutschen Bundespost im Rahmen seiner Aufgabenstellung nach den §§ 9 bis 11 des Postverfassungsgesetzes sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.

(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre Dateien haben sie schriftlich festzulegen:

1. Bezeichnung und Art der Dateien,
2. Zweckbestimmung,
3. Art der gespeicherten Daten,
4. betroffenen Personenkreis,
5. Art der regelmäßig zu übermittelnden Daten und deren Empfänger,
6. Regelfristen für die Löschung der Daten,
7. zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind.

Sie haben ferner dafür zu sorgen, daß die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, überwacht wird.

(3) Absatz 2 Satz 2 gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.

ZWEITER UNTERABSCHNITT

Rechte des Betroffenen

§ 19

Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft oder Empfänger dieser Daten beziehen, und
2. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten in Akten gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muß.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Falle ist der Betroffene darauf hinzuweisen, daß er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

§ 20

Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, daß personenbezogene Daten in Akten unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) Personenbezogene Daten in Dateien sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder
2. ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten in Dateien sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

(5) Personenbezogene Daten in Akten sind zu sperren, wenn die Behörde im Einzelfall feststellt, daß ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(6) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerläßlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer regelmäßigen Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

(8) § 2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

§ 21

Anrufung des Bundesbeauftragten für den Datenschutz

Jedermann kann sich an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

DRITTER UNTERABSCHNITT

Bundesbeauftragter für den Datenschutz

§ 22

Wahl des Bundesbeauftragten für den Datenschutz

(1) Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Der Bundesbeauftragte muß bei seiner Wahl das 35. Lebensjahr vollendet haben. Der Gewählte ist vom Bundespräsidenten zu ernennen.

(2) Der Bundesbeauftragte leistet vor dem Bundesminister des Innern folgenden Eid:

„Ich schwöre, daß ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe.“

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

(4) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen Amtsverhältnis. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Rechtsaufsicht der Bundesregierung.

(5) Der Bundesbeauftragte wird beim Bundesminister des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministers des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministers des Innern in einem eigenen Kapitel auszuweisen. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden.

(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.

§ 23

**Rechtsstellung des Bundesbeauftragten
für den Datenschutz**

(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz beginnt mit der Aushändigung der Ernennungsurkunde. Es endet

1. mit Ablauf der Amtszeit,
2. mit der Entlassung.

Der Bundespräsident entläßt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Falle der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.

(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) Der Bundesbeauftragte hat dem Bundesminister des Innern Mitteilung über Geschenke zu machen, die er in bezug auf sein Amt erhält. Der Bundesminister des Innern entscheidet über die Verwendung der Geschenke.

(4) Der Bundesbeauftragte ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, daß über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.

(5) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministers des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten.

(6) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. § 28 des Gesetzes über das Bundesverfassungsgericht in der Fassung der Bekanntmachung vom 12. Dezember 1985 (BGBl. I S. 2229) bleibt unberührt.

(7) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluß des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 9 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im übrigen sind die §§ 13 bis 20 des Bundesministergesetzes in der Fassung der Bekanntmachung vom 27. Juli 1971 (BGBl. I S. 1166), zuletzt geändert durch das Gesetz zur Kürzung des Amtsgehalts der Mitglieder der Bundesregierung und der Parlamentarischen Staatssekretäre vom 22. Dezember 1982 (BGBl. I S. 2007), mit der Maßgabe anzuwenden, daß an die Stelle der zweijährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittelbar vor seiner Wahl zum Bundesbeauftragten als Beamter oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 9 zu durchlaufenden Amt befunden hat.

§ 24

**Kontrolle durch den Bundesbeauftragten
für den Datenschutz**

(1) Der Bundesbeauftragte für den Datenschutz kontrolliert bei den öffentlichen Stellen des Bundes, unbeschadet der ihnen bei der Erfüllung ihrer Aufgaben obliegenden fachlichen Beurteilung und Verantwortlichkeit, die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz. Werden personenbezogene Daten in Akten verarbeitet oder genutzt, kontrolliert der Bundesbeauftragte die Erhebung, Verarbeitung oder Nutzung, wenn der Betroffene ihm hinreichende Anhaltspunkte dafür darlegt, daß er dabei in seinen Rechten verletzt worden ist, oder dem Bundesbeauftragten hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen; die Kontrolle ist auf den Einzelfall beschränkt.

auftragten hinreichende Anhaltspunkte für eine derartige Verletzung vorliegen; die Kontrolle ist auf den Einzelfall beschränkt.

(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. Das Post- und Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird eingeschränkt, soweit dies zur Ausübung der Kontrolle bei den speichernden Stellen der Deutschen Bundespost erforderlich ist. Das Kontrollrecht erstreckt sich mit Ausnahme von Nummer 4 nicht auf den Inhalt des Post- und Fernmeldeverkehrs.

Der Kontrolle durch den Bundesbeauftragten unterliegen nicht:

1. personenbezogene Daten, die der Kontrolle durch die Kommission nach § 9 des Gesetzes zu Artikel 10 GG unterliegen, es sei denn, die Kommission untersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten, und

2. a) personenbezogene Daten, die dem Post- und Fernmeldegeheimnis nach Artikel 10 des Grundgesetzes unterliegen,

b) personenbezogene Daten, die dem Steuergeheimnis nach § 30 der Abgabenordnung oder dem Arztgeheimnis unterliegen und

c) personenbezogene Daten in Personalakten oder in den Akten über die Sicherheitsüberprüfung,

wenn der Betroffene der Kontrolle im Einzelfall gegenüber dem Bundesbeauftragten für den Datenschutz widerspricht.

(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,

2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in § 4 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, daß die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 25 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 25

Beanstandungen durch den Bundesbeauftragten für den Datenschutz

(1) Stellt der Bundesbeauftragte für den Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,

2. bei der Bundesbahn gegenüber dem Vorstand,

3. bei der Deutschen Bundespost gegenüber den Vorständen der Unternehmen oder gegenüber dem Direktorium im Rahmen seiner Aufgabenstellung nach den §§ 9 bis 11 des Postverfassungsgesetzes,

4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 4 unterrichtet der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

§ 26

Weitere Aufgaben des Bundesbeauftragten für den Datenschutz; Datenregister

(1) Der Bundesbeauftragte für den Datenschutz erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. Der Tätigkeitsbericht soll auch eine Darstellung der wesentlichen Entwicklung des Datenschutzes im nicht-öffentlichen Bereich enthalten.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin.

(5) Der Bundesbeauftragte führt ein Register der automatisiert geführten Dateien, in denen personenbezogene Daten gespeichert werden. Das gilt nicht für die Dateien der in § 19 Abs. 3 genannten Behörden sowie für Dateien nach § 18 Abs. 3. Die öffentlichen Stellen, deren Dateien in das Register aufgenommen werden, sind verpflichtet, dem Bundesbeauftragten eine Übersicht gemäß § 18 Abs. 2 Satz 2 Nr. 1 bis 6 zuzuleiten. Das Register kann von jedermann eingesehen werden. Die Angaben nach § 18 Abs. 2 Satz 2 Nr. 3 und 5 über Dateien der in § 6 Abs. 2 und § 17 Abs. 3 genannten Behörden unterliegen nicht der Einsichtnahme. Der Bundesbeauftragte kann im Einzelfall für andere öffentliche Stellen mit deren Einverständnis festlegen, daß einzelne Angaben nicht der Einsichtnahme unterliegen.

DRITTER ABSCHNITT

Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

ERSTER UNTERABSCHNITT

Rechtsgrundlagen der Datenverarbeitung

§ 27

Anwendungsbereich *Grundnutzung*

(1) Die Vorschriften dieses Abschnittes gelten für die Verarbeitung personenbezogener Daten, soweit die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeitet oder genutzt werden, durch

1. nicht-öffentliche Stellen,
2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
- b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.

In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.

(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten in Akten, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer Datei entnommen worden sind.

§ 28

Datenspeicherung, -übermittlung und -nutzung für eigene Zwecke

(1) Das Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen,
2. soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt,
3. wenn die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung offensichtlich überwiegt.

4. wenn es zur Durchführung wissenschaftlicher Forschung im Interesse der speichernden Stelle erforderlich ist und das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt. Dies gilt nicht, wenn der Zweck der Forschung durch die Verwendung anonymisierter Daten erreicht werden kann.

(2) Die Übermittlung oder Nutzung ist auch zulässig

1. a) soweit es zur Wahrung berechtigter Interessen eines Dritten oder öffentlicher Interessen erforderlich ist oder
- b) wenn es sich um listenmäßig oder sonst zusammengefaßte Daten über Angehörige einer Personengruppe handelt, die sich auf

- eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
- Berufs-, Branchen- oder Geschäftsbezeichnung,
- Namen,
- Titel,
- akademische Grade,
- Anschrift,

- Geburtsjahr

beschränken und

2. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat. In den Fällen der Nummer 1 Buchstabe b kann im allgemeinen davon ausgegangen werden, daß dieses Interesse besteht, wenn im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses gespeicherte Daten übermittelt werden sollen, die sich
 - auf gesundheitliche Verhältnisse,
 - auf strafbare Handlungen,
 - auf Ordnungswidrigkeiten,
 - auf religiöse oder politische Anschauungen sowie
 - bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse beziehen.

3. wenn es zur Durchführung wissenschaftlicher Forschung im Interesse einer Forschungseinrichtung erforderlich ist und das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt. Dies gilt nicht, wenn der Zweck der Forschung durch die Verwendung anonymisierter Daten erreicht werden kann.

(3) Widerspricht der Betroffene bei der speichernden Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig. Widerspricht der Betroffene beim Empfänger der nach Absatz 2 übermittelten Daten der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren.

(4) Werden personenbezogene Daten zur Wahrung berechtigter Interessen eines Dritten (Absatz 2 Nr. 1 Buchstabe a) übermittelt, darf der Empfänger diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt worden sind. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen der Absätze 1 und 2 zulässig. Die übermittelnde Stelle hat den Empfänger darauf hinzuweisen.

§ 28

Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung

(1) Das geschäftsmäßige Speichern oder Verändern personenbezogener Daten zum Zwecke der Übermittlung ist zulässig, wenn

1. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Speicherung oder Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Speicherung oder Veränderung offensichtlich überwiegt.

(2) Die Übermittlung ist zulässig, wenn

1. a) der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat oder
- b) es sich um listenmäßig oder sonst zusammengefaßte Daten nach § 28 Abs. 2 Nr. 1 Buchstabe b handelt, die für Zwecke der Werbung oder der Markt- oder Meinungsforschung übermittelt werden sollen, und
2. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat.

§ 28 Abs. 2 ^{Nr. 2} Satz 2 gilt entsprechend.

Bei der Übermittlung nach Nummer 1 Buchstabe a sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Empfänger.

(3) Für die Verarbeitung oder Nutzung der nach Absatz 2 Nr. 1 Buchstabe a übermittelten Daten gilt § 28 Abs. 3 und 4.

§ 30

Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung in anonymisierter Form

(1) Werden personenbezogene Daten geschäftsmäßig gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zweckes der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Veränderung hat, oder
2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Veränderung offensichtlich überwiegt.

(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) Die §§ 22, 33 und 35 gelten nicht.

§ 31

Besondere Zweckbindung ^{Schutz}

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§ 32

Meldepflichten

(1) Die Stellen, die personenbezogene Daten geschäftsmäßig

1. zum Zwecke der Übermittlung speichern,
2. zum Zwecke der anonymisierten Übermittlung speichern oder
3. im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen,

sowie ihre Zweigniederlassungen und unselbständigen Zweigstellen haben die Aufnahme und Beendigung ihrer Tätigkeit der zuständigen Aufsichtsbehörde innerhalb eines Monats mitzuteilen.

(2) Bei der Anmeldung sind folgende Angaben für das bei der Aufsichtsbehörde geführte Register mitzuteilen:

1. Name oder Firma der Stelle,
2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzlich oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift,
4. Geschäftszwecke der Stelle und der Datenverarbeitung,
5. Name des Beauftragten für den Datenschutz,
6. allgemeine Beschreibung der Art der gespeicherten personenbezogenen Daten. Im Falle des Absatzes 1 Nr. 3 ist diese Angabe nicht erforderlich.

(3) Bei der Anmeldung sind außerdem folgende Angaben mitzuteilen, die nicht in das Register aufgenommen werden:

1. Art der eingesetzten Datenverarbeitungsanlagen,
2. bei regelmäßiger Übermittlung personenbezogener Daten Empfänger und Art der übermittelten Daten.

(4) Absatz 1 gilt für die Änderung der nach Absätzen 2 und 3 mitgeteilten Angaben entsprechend.

(5) Die Aufsichtsbehörde kann im Einzelfall festlegen, welche Angaben nach Absatz 2 Nr. 4 und 6, Absatz 3 und Absatz 4 mitgeteilt werden müssen. Der mit den Mitteilungen verbundene Aufwand muß in einem angemessenen Verhältnis zu ihrer Bedeutung für die Überwachung durch die Aufsichtsbehörde stehen.

ZWEITER UNTERABSCHNITT

Rechte des Betroffenen

§ 33

Benachrichtigung des Betroffenen

(1) Werden erstmals personenbezogene Daten für eigene Zwecke gespeichert, ist der Betroffene von der Speicherung und der Art der Daten zu benachrichtigen.

gen. Werden personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, ist der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Daten nur deshalb gespeichert sind, weil sie auf Grund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen,
3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,
4. die zuständige öffentliche Stelle gegenüber der speichernden Stelle festgestellt hat, daß das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
5. die Daten in einer Datei gespeichert werden, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht wird,
6. die Daten für eigene Zwecke gespeichert sind und
 - a) aus allgemein zugänglichen Quellen entnommen sind oder
 - b) die Benachrichtigung die Geschäftszwecke der speichernden Stelle erheblich gefährden würde, es sei denn, daß das Interesse an der Benachrichtigung die Gefährdung überwiegt, oder
7. die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und
 - a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder
 - b) es sich um listenmäßig oder sonst zusammengefaßte Daten handelt (§ 29 Abs. 2 Nr. 1 Buchstabe b).

§ 34

Auskunft an den Betroffenen

(1) Der Betroffene kann Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf Herkunft und Empfänger beziehen,
2. den Zweck der Speicherung und
3. Personen und Stellen, an die seine Daten regelmäßig übermittelt werden, wenn seine Daten automatisiert verarbeitet werden.

Er soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann der Betroffene über Herkunft und Empfänger nur Auskunft verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. In diesem Falle ist Auskunft über Herkunft und Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind.

(2) Der Betroffene kann von Stellen, die geschäftsmäßig personenbezogene Daten zum Zwecke der Auskunftserteilung speichern, Auskunft über seine personenbezogenen Daten verlangen, auch wenn sie nicht in einer Datei gespeichert sind. Auskunft über Herkunft und Empfänger kann der Betroffene nur verlangen, wenn er begründete Zweifel an der Richtigkeit der Daten geltend macht. § 38 Abs. 1 ist mit der Maßgabe anzuwenden, daß die Aufsichtsbehörde im Einzelfall die Einhaltung von Satz 1 überprüft, wenn der Betroffene begründet darlegt, daß die Auskunft nicht oder nicht richtig erteilt worden ist.

(3) Die Auskunft wird schriftlich erteilt, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(4) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Nr. 2 bis 6 nicht zu benachrichtigen ist.

(5) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert, kann jedoch ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen direkt zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann in den Fällen nicht verlangt werden, in denen besondere Umstände die Annahme rechtfertigen, daß Daten unrichtig oder unzulässig gespeichert werden, oder in denen die Auskunft ergibt, daß die Daten zu berichtigen oder unter der Voraussetzung des § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(6) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten und Angaben zu verschaffen. Er ist hierauf in geeigneter Weise hinzuweisen.

§ 35

Berichtigung, Löschung und Sperrung von Daten

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

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,
2. es sich um Daten über gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten sowie religiöse oder politische Anschauungen handelt und ihre Richtigkeit von der speichernden Stelle nicht bewiesen werden kann,
3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zweckes der Speicherung nicht mehr erforderlich ist, oder

4. sie geschäftsmäßig zum Zwecke der Übermittlung verarbeitet werden und eine Prüfung am Ende des fünften Kalenderjahres nach ihrer erstmaligen Speicherung ergibt, daß eine längerwährende Speicherung nicht erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Falle des Absatzes 2 Nr. 3 oder 4 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,
2. Grund zu der Annahme besteht, daß durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen läßt.

(5) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(6) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer regelmäßigen Datenübermittlung diese Daten zur Speicherung weitergegeben werden, wenn dies zur Wahrung der schutzwürdigen Interessen des Betroffenen erforderlich ist.

(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der speichernden Stelle oder eines Dritten liegenden Gründen unerlässlich ist und
2. die Daten hierfür übermittelt oder genutzt werden dürfen, wenn sie nicht gesperrt wären.

DRITTER UNTERABSCHNITT

Beauftragter für den Datenschutz, Aufsichtsbehörde

§ 36

Bestellung eines Beauftragten für den Datenschutz

(1) Die nicht-öffentlichen Stellen, die personenbezogene Daten automatisiert verarbeiten und damit in der Regel mindestens fünf Arbeitnehmer ständig beschäftigen, haben spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit einen Beauftragten für den Datenschutz schriftlich zu bestellen. Das gleiche gilt, wenn personenbezogene Daten auf andere Weise verarbeitet werden und damit in der Regel mindestens zwanzig Arbeitnehmer ständig beschäftigt sind.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt.

(3) Der Beauftragte für den Datenschutz ist dem Inhaber, dem Vorstand, dem Geschäftsführer oder dem sonstigen gesetzlich oder nach der Verfassung des Unternehmens berufenen Leiter unmittelbar zu unterstellen. Er ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann nur auf Verlangen der Aufsichtsbehörde oder in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches widerrufen werden.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(5) Die nicht-öffentliche Stelle hat den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

§ 37

Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz hat die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. Zu diesem Zweck kann er sich in Zweifelsfällen an die Aufsichtsbehörde wenden. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben

der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen 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,

3. bei der Auswahl der bei der Verarbeitung personenbezogener Daten tätigen Personen beratend mitzuwirken.

(2) Dem Beauftragten ist von der nicht-öffentlichen Stelle eine Übersicht zur Verfügung zu stellen über

1. eingesetzte Datenverarbeitungsanlagen,
2. Bezeichnung und Art der Dateien,
3. Art der gespeicherten Daten,
4. Geschäftszwecke, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,
5. deren regelmäßige Empfänger,
6. zugriffsberechtigte Personengruppen oder Personen, die allein zugriffsberechtigt sind.

(3) Absatz 2 Nr. 2 bis 6 gilt nicht für Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden.

§ 38

Aufsichtsbehörde

(1) Die Aufsichtsbehörde überprüft im Einzelfall die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, wenn ihr hinreichende Anhaltspunkte dafür vorliegen, daß eine dieser Vorschriften durch nicht-öffentliche Stellen verletzt ist, insbesondere wenn es der Betroffene selbst begründet darlegt.

(2) Werden personenbezogene Daten geschäftsmäßig

1. zum Zwecke der Übermittlung gespeichert,
2. zum Zwecke der anonymisierten Übermittlung gespeichert oder
3. im Auftrag durch Dienstleistungsunternehmen verarbeitet,

überwacht die Aufsichtsbehörde die Ausführung dieses Gesetzes oder anderer Vorschriften über den Da-

tenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln. Die Aufsichtsbehörde führt das Register nach § 32 Abs. 2. Das Register kann von jedem eingesehen werden.

(3) Die der Prüfung unterliegenden Stellen sowie 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. Der Auskunftspflichtige ist darauf hinzuweisen.

(4) Die von der Aufsichtsbehörde mit der Überprüfung oder Überwachung beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 37 Abs. 2 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 gilt entsprechend. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.

(5) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, kann die Aufsichtsbehörde anordnen, daß im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Überwachung der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.

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

VIERTER ABSCHNITT

Sondervorschriften

§ 39

Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der speichernden Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muß die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

§ 40

Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die Übermittlung personenbezogener Daten an andere als öffentliche Stellen für Zwecke der wissenschaftlichen Forschung ist nur zulässig, wenn diese sich verpflichten, die übermittelten Daten nicht für andere Zwecke zu verarbeiten oder zu nutzen und die Vorschrift des Absatzes 3 einzuhalten.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(4) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder
2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 41

Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) Soweit personenbezogene Daten von Unternehmen oder Hilfsunternehmen der Presse oder des Films oder von Hilfsunternehmen des Rundfunks ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet oder genutzt werden, gelten von den Vorschriften dieses Gesetzes nur die §§ 5 und 9. Soweit Verlage personenbezogene Daten zur Herausgabe von Adressen-, Telefon-, Branchen- oder vergleichbaren Verzeichnissen verarbeiten oder nutzen, gilt Satz 1 nur, wenn mit der Herausgabe zugleich eine journalistisch-redaktionelle Tätigkeit verbunden ist.

(2) Führt die journalistisch-redaktionelle Verarbeitung oder Nutzung personenbezogener Daten durch die Rundfunkanstalten des Bundesrechts zur Veröffentlichung von Gegendarstellungen der Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Rundfunkanstalten des Bundesrechts in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrundeliegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann verweigert werden, soweit aus den Daten auf die Person des Verfassers, Einsenders oder Gewährsmannes von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann. Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im übrigen gelten für die Rundfunkanstalten des Bundesrechts von den Vorschriften dieses Gesetzes die §§ 5 und 9. Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

§ 42

Datenschutzbeauftragte der Rundfunkanstalten des Bundesrechts

(1) Die Rundfunkanstalten des Bundesrechts bestellen jeweils einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz tritt. Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Im übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) Jedermann kann sich entsprechend § 21 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) Der Beauftragte für den Datenschutz erstattet den Organen der jeweiligen Rundfunkanstalt des Bundesrechts alle zwei Jahre, erstmals zum 1. Januar . . . einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluß eines Organes der jeweiligen Rundfunkanstalt. Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz.

(5) Weitere Regelungen entsprechend den §§ 23 bis 26 treffen die Rundfunkanstalten des Bundesrechts jeweils für ihren Bereich. § 18 bleibt unberührt.

FÜNFTER ABSCHNITT

Schlußvorschriften

§ 43

Strafvorschriften

(1) Wer unbefugt personenbezogene Daten, die die Voraussetzung des § 1 Abs. 2 oder 3 erfüllen und die nicht offenkundig sind,

1. speichert, verändert oder übermittelt,
2. zum Abruf mittels automatisierten Verfahrens bereithält oder
3. abrufen oder sich oder einem anderen aus Dateien verschafft,

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

(2) Ebenso wird bestraft, wer

1. die Übermittlung von personenbezogenen Daten, die die Voraussetzung des § 1 Abs. 2 oder 3 erfüllen und die nicht offenkundig sind, durch unrichtige Angaben erschleicht,

2. entgegen § 16 Abs. 4 Satz 1 oder § 28 Abs. 4 Satz 1, auch in Verbindung mit § 29 Abs. 3, oder § 40 Abs. 1 die übermittelten Daten für andere Zwecke nutzt, indem er sie an Dritte weitergibt, oder
3. entgegen § 30 Abs. 1 Satz 2 die in § 30 Abs. 1 Satz 1 bezeichneten Merkmale oder entgegen § 40 Abs. 3 Satz 3 die in § 40 Abs. 3 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt.

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

(4) Die Tat wird nur auf Antrag verfolgt.

§ 44

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 29 Abs. 2 Satz 2 oder 3 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,
2. entgegen § 32 Abs. 1, auch in Verbindung mit Absatz 4, eine Meldung nicht oder nicht rechtzeitig erstattet oder entgegen § 32 Abs. 2, auch in Verbindung mit Absatz 4, bei einer solchen Meldung die erforderlichen Angaben nicht, nicht richtig oder nicht vollständig mitteilt,
3. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,
4. entgegen § 35 Abs. 5 Satz 3 Daten ohne Gegendarstellung übermittelt,
5. entgegen § 36 Abs. 1 einen Beauftragten für den Datenschutz nicht oder nicht rechtzeitig bestellt,
6. entgegen § 38 Abs. 3 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 38 Abs. 4 Satz 4 den Zutritt zu den Grundstücken oder Geschäftsräumen oder die Vornahme von Prüfungen oder Besichtigungen oder die Einsicht in geschäftliche Unterlagen nicht duldet, oder
7. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

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

§ 45

Berlin-Klausel

Dieses Gesetz gilt nach Maßgabe des § 13 Abs. 1 des Dritten Überleitungsgesetzes auch im Land Berlin.

Anlage zu § 9 Satz 1

Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

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

Artikel 2

Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (Bundesverfassungsschutzgesetz – BVerfSchG –)

ERSTER ABSCHNITT

Zusammenarbeit, Aufgaben der Verfassungsschutzbehörden

§ 1

Zusammenarbeitspflicht

(1) Der Verfassungsschutz dient dem Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes und der Länder.

(2) Der Bund und die Länder sind verpflichtet, in Angelegenheiten des Verfassungsschutzes zusammenzuarbeiten.

(3) Die Zusammenarbeit besteht auch in gegenseitiger Unterstützung und Hilfeleistung.

§ 2

Verfassungsschutzbehörden

(1) Für die Zusammenarbeit des Bundes mit den Ländern unterhält der Bund ein Bundesamt für Verfassungsschutz als Bundesoberbehörde. Es untersteht

dem Bundesminister des Innern. Das Bundesamt für Verfassungsschutz darf einer polizeilichen Dienststelle nicht angegliedert werden.

(2) Für die Zusammenarbeit der Länder mit dem Bund und der Länder untereinander unterhält jedes Land eine Behörde zur Bearbeitung von Angelegenheiten des Verfassungsschutzes.

§ 3

Aufgaben der Verfassungsschutzbehörden

(1) Aufgabe der Verfassungsschutzbehörden des Bundes und der Länder ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane des Bundes oder eines Landes oder ihrer Mitglieder zum Ziele haben,

2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht,

3. Bestrebungen im Geltungsbereich dieses Gesetzes, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen auswärtige Belange der Bundesrepublik Deutschland gefährden.

(2) Bestrebungen gegen die freiheitliche demokratische Grundordnung sind ziel- und zweckgerichtete Verhaltensweisen oder Betätigungen in der Regel in oder für Zwecke einer Organisation oder einer unorganisierten Gruppierung gegen dieses Schutzgut. Voraussetzung für die Sammlung und Auswertung von Informationen im Sinne des Absatzes 1 ist das Vorliegen tatsächlicher Anhaltspunkte.

(3) Die Verfassungsschutzbehörden des Bundes und der Länder wirken mit

1. bei der Sicherheitsüberprüfung von Personen, denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können,

2. bei der Sicherheitsüberprüfung von Personen, die an sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen beschäftigt sind oder werden sollen,

3. bei technischen Sicherheitsmaßnahmen zum Schutz von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen gegen die Kenntnismahme durch Unbefugte.

Besteht die Sicherheitsüberprüfung des Bundesamtes für Verfassungsschutz nach Satz 1 lediglich in der Auswertung bereits vorhandenen Wissens der Beschäftigungsstelle, der Strafverfolgungs- oder Sicherheitsbehörden, ist es erforderlich und ausreichend, daß der Betroffene und die in die Sicherheitsüberprüfung einzubeziehenden Personen von der Einleitung der Überprüfung Kenntnis haben; im übrigen ist die Zustimmung erforderlich, soweit gesetzlich nichts anderes bestimmt ist.

In die Sicherheitsüberprüfung dürfen der Ehegatte, Verlobte oder die Person, die mit dem Betroffenen in eheähnlicher Gemeinschaft lebt, miteinbezogen werden.

(4) Die Verfassungsschutzbehörden sind an die allgemeinen Rechtsvorschriften gebunden (Artikel 20 des Grundgesetzes).

§ 4

Gegenseitige Unterrichtung der Verfassungsschutzbehörden

(1) Die Verfassungsschutzbehörden unterrichten einander über alle Angelegenheiten, deren Kenntnis zur Erfüllung ihrer Aufgaben erforderlich ist.

(2) Die Verfassungsschutzbehörden sind verpflichtet, beim Bundesamt für Verfassungsschutz zur Erfüllung der Unterrichtungspflichten nach Absatz 1 gemeinsame Dateien zu führen, die sie im automatisierten Verfahren nutzen. Diese Dateien enthalten nur die Daten, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Die Speicherung personenbezogener Daten ist nur unter den Voraussetzungen der §§ 8 und 9 zulässig. Der Abruf im automatisierten Verfahren durch andere Stellen ist nicht zulässig. Die Verantwortung einer speichernden Stelle im Sinne der allgemeinen Vorschriften des Datenschutzrechts trägt jede Verfassungsschutzbehörde nur für die von ihr eingegebenen Daten; nur sie darf diese Daten verändern, sperren oder löschen. Die eingebende Stelle muß feststellbar sein. Das Bundesamt für Verfassungsschutz trifft für die gemeinsamen Dateien die technischen und organisatorischen Maßnahmen nach § 8 des Bundesdatenschutzgesetzes. Die Führung von Textdateien oder Dateien, die weitere als die in Satz 2 genannten Daten enthalten, ist unter den Voraussetzungen dieses Absatzes nur zulässig für eng umgrenzte Anwendungsgebiete zur Aufklärung von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht oder von Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten. Die Zugriffsberechtigung ist auf Personen zu beschränken, die unmittelbar mit Arbeiten in diesem Anwendungsgebiet betraut sind; in der Dateianordnung (§ 12) ist die Erforderlichkeit der Aufnahme von Textzusätzen in der Datei zu begründen.

§ 5

Weisungsrechte des Bundes

Die Bundesregierung kann, wenn ein Angriff auf die verfassungsmäßige Ordnung des Bundes erfolgt, den obersten Landesbehörden die für die Zusammenarbeit der Länder mit dem Bund auf dem Gebiete des Verfassungsschutzes erforderlichen Weisungen erteilen.

ZWEITER ABSCHNITT

Bundesamt für Verfassungsschutz

§ 6

Befugnisse des Bundesamtes für Verfassungsschutz

(1) Das Bundesamt für Verfassungsschutz darf die zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten erheben, verarbeiten und nutzen, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen in diesem Gesetz entgegenstehen.

(2) Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen anwenden. Diese sind in einer Dienstvorschrift zu benennen, die auch die Zuständigkeit für die Anordnung solcher Informationsbeschaffungen regelt. Die Dienstvorschrift bedarf der Zustimmung des Bundesministers des Innern, der die Parlamentarische Kontrollkommission, unterrichtet.

(3) Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Bundesamt für Verfassungsschutz nicht zu; es darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen es selbst nicht befugt ist.

(4) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck anzugeben. Der Betroffene ist auf die Freiwilligkeit seiner Angaben und bei einer Sicherheitsüberprüfung nach § 3 Abs. 3 auf eine dienst-, arbeitsrechtliche oder sonstige vertragliche Mitwirkungspflicht hinzuweisen.

(5) Von mehreren geeigneten Maßnahmen hat das Bundesamt für Verfassungsschutz diejenige zu wählen, die den Betroffenen voraussichtlich am wenigsten beeinträchtigt. Eine Maßnahme darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

§ 7

Besondere Formen der Datenerhebung

(1) Das Bundesamt für Verfassungsschutz darf Informationen, insbesondere personenbezogene Daten, mit den Mitteln gemäß § 6 Abs. 2 erheben, wenn Tatsachen die Annahme rechtfertigen, daß

1. auf diese Weise Erkenntnisse über Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 oder die zur Erforschung solcher Erkenntnisse erforderlichen Quellen gewonnen werden können oder
2. dies zum Schutz der Mitarbeiter, Einrichtungen, Gegenstände und Quellen des Bundesamtes für Verfassungsschutz gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten erforderlich ist.

Die Erhebung nach Satz 1 ist unzulässig, wenn die Erforschung des Sachverhalts auf andere, den Betroffenen weniger beeinträchtigende Weise möglich ist; eine geringere Beeinträchtigung ist in der Regel anzunehmen, wenn die Information aus allgemein zugänglichen Quellen oder durch eine Auskunft nach § 16 Abs. 3 gewonnen werden kann. Die Anwendung eines Mittels gemäß § 6 Abs. 2 darf nicht erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhaltes stehen. Die Maßnahme ist unverzüglich zu beenden, wenn ihr Zweck erreicht ist oder sich Anhaltspunkte dafür ergeben, daß er nicht oder nicht auf diese Weise erreicht werden kann.

(2) Das in einer Wohnung nicht öffentlich gesprochene Wort darf mit technischen Mitteln nur heimlich mitgehört oder aufgezeichnet werden, wenn es im Einzelfall zur Abwehr einer gegenwärtigen gemeinen Gefahr oder einer gegenwärtigen Lebensgefahr für einzelne Personen unerlässlich ist und geeignete polizeiliche Hilfe für das bedrohte Rechtsgut nicht rechtzeitig erlangt werden kann.

Satz 1 gilt entsprechend für einen verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen und Bildaufzeichnungen.

(3) Bei Erhebungen nach Absatz 2 und solchen nach Absatz 1, die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen, wozu insbesondere das Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem verdeckten Einsatz technischer Mittel gehören, ist

1. der Eingriff nach seiner Beendigung dem Betroffenen mitzuteilen, sobald eine Gefährdung des Zweckes des Eingriffs ausgeschlossen werden kann, und
2. die Parlamentarische Kontrollkommission zu unterrichten.

Die durch solche Maßnahmen erhobenen Informationen dürfen nur nach Maßgabe des § 7 Abs. 3 des Gesetzes zu Artikel 10 Grundgesetz verwendet werden.

§ 8

**Speicherung, Veränderung und Nutzung
personenbezogener Daten**

(1) Das Bundesamt für Verfassungsschutz darf zur Erfüllung seiner Aufgaben personenbezogene Daten in Dateien speichern, verändern und nutzen, wenn

1. tatsächliche Anhaltspunkte für Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 vorliegen,
2. dies für die Erforschung und Bewertung von Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 erforderlich ist oder
3. das Bundesamt für Verfassungsschutz nach § 3 Abs. 3 tätig wird.

(2) Zur Aufgabenerfüllung nach § 3 Abs. 3 dürfen in automatisierten Dateien nur personenbezogene Daten über die Personen gespeichert werden, die der Sicherheitsüberprüfung unterliegen oder in die Sicherheitsüberprüfung einbezogen werden.

(3) Das Bundesamt für Verfassungsschutz hat die Speicherdauer auf das für seine Aufgabenerfüllung erforderliche Maß zu beschränken.

§ 9

**Speicherung, Veränderung und Nutzung
personenbezogener Daten von Minderjährigen**

(1) Das Bundesamt für Verfassungsschutz darf unter den Voraussetzungen des § 8 Daten über Minderjährige vor Vollendung des 16. Lebensjahres in zu ihrer Person geführten Akten nur speichern, verändern und nutzen, wenn tatsächliche Anhaltspunkte dafür bestehen, daß der Minderjährige eine der in § 2 des Gesetzes zu Artikel 10 Grundgesetz genannten Straftaten plant, begeht oder begangen hat. In Dateien ist eine Speicherung von Daten oder über das Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres nicht zulässig.

(2) In Dateien gespeicherte Daten über Minderjährige sind nach zwei Jahren auf die Erforderlichkeit der Speicherung zu überprüfen und spätestens nach fünf Jahren zu löschen, es sei denn, daß nach Eintritt der Volljährigkeit weitere Erkenntnisse nach § 3 Abs. 1 angefallen sind.

§ 10

**Berichtigung, Löschung und Sperrung
von personenbezogenen Daten in Dateien**

(1) Das Bundesamt für Verfassungsschutz hat die in Dateien gespeicherten personenbezogenen Daten zu berichtigen, wenn sie unrichtig sind.

(2) Das Bundesamt für Verfassungsschutz hat die in Dateien gespeicherten personenbezogenen Daten zu löschen, wenn ihre Speicherung unzulässig war oder ihre Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist. Die Löschung unterbleibt, wenn Grund zu der Annahme besteht, daß durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden. In diesem Falle sind die Daten zu sperren. Sie dürfen nur noch mit Einwilligung des Betroffenen übermittelt werden.

(3) Das Bundesamt für Verfassungsschutz prüft bei der Einzelfallbearbeitung und nach festgesetzten Fristen, ob gespeicherte personenbezogene Daten zu berichtigen oder zu löschen sind.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§ 11

**Berichtigung und Sperrung
personenbezogener Daten in Akten**

(1) Stellt das Bundesamt für Verfassungsschutz fest, daß in Akten gespeicherte personenbezogene Daten unrichtig sind oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

(2) Das Bundesamt für Verfassungsschutz hat personenbezogene Daten zu sperren, wenn es im Einzelfall feststellt, daß ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für seine künftige Aufgabenerfüllung nicht mehr erforderlich sind. Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr genutzt oder übermittelt werden. Eine Aufhebung der Sperrung ist möglich, wenn ihre Voraussetzungen nachträglich entfallen.

§ 12

Dateianordnungen

(1) Für jede automatisierte Datei beim Bundesamt für Verfassungsschutz nach § 4 Abs. 2 oder § 8 sind in einer Dateianordnung, die der Zustimmung des Bundesministers des Innern bedarf, festzulegen:

1. Bezeichnung der Datei,
2. Zweck der Datei,
3. Voraussetzungen der Speicherung, Übermittlung und Nutzung (betroffener Personenkreis, Arten der Daten),
4. Anlieferung oder Eingabe,
5. Zugangsberechtigung,
6. Überprüfungsfristen, Speicherdauer,
7. Protokollierung.

Der Bundesbeauftragte für den Datenschutz ist vor Erlass einer Dateianordnung anzuhören.

(2) Die Speicherung personenbezogener Daten ist auf das erforderliche Maß zu beschränken. In angemessenen Abständen ist die Notwendigkeit der Weiterführung oder Änderung der Dateien zu überprüfen.

§ 13

Auskunft an den Betroffenen

(1) Das Bundesamt für Verfassungsschutz erteilt dem Betroffenen über zu seiner Person gespeicherte Daten auf Antrag unentgeltlich Auskunft, soweit er hierzu auf einen konkreten Sachverhalt hinweist und ein besonderes Interesse an einer Auskunft darlegt.

(2) Die Auskunftserteilung unterbleibt, soweit

1. eine Gefährdung der Aufgabenerfüllung durch die Auskunftserteilung zu besorgen ist,
2. durch die Auskunftserteilung Quellen gefährdet sein können oder die Ausforschung des Erkenntnisstandes oder der Arbeitsweise des Bundesamtes für Verfassungsschutz zu befürchten ist,
3. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder
4. die Daten oder die Tatsache der Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen.

(3) Die Auskunftsverpflichtung erstreckt sich nicht auf die Herkunft der Daten und die Empfänger von Übermittlungen.

(4) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung. Wird die Auskunftserteilung abgelehnt, ist der Betroffene auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinzuweisen, daß er sich an den Bundesbeauftragten für den Datenschutz wenden kann. Dem Bundesbeauftragten für den Datenschutz ist auf sein Verlangen Auskunft zu erteilen, soweit nicht der Bundesminister des Innern im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Mitteilungen des Bundesbeauftragten an den Betroffenen dürfen keine Rückschlüsse auf den Erkenntnisstand des Bundesamtes für Verfassungsschutz zulassen, sofern es nicht einer weitergehenden Auskunft zustimmt.

§ 14

Berichtspflicht des Bundesamtes für Verfassungsschutz

(1) Das Bundesamt für Verfassungsschutz unterrichtet den Bundesminister des Innern über seine Tätigkeit.

(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch den Bundesminister des Innern über Bestrebungen und Tätigkeiten nach § 3 Abs. 1, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. Dabei dürfen auch personenbezogene Daten bekanntgegeben werden, wenn die Bekanntgabe für das Verständnis des Zusammenhanges oder der Darstellung von Organisationen oder unorganisierten Gruppierungen erforderlich ist und die Interessen der Allgemeinheit das schutzwürdige Interesse des Betroffenen überwiegen.

In dem Bericht sind die Zuschüsse des Bundeshaushaltes an das Bundesamt für Verfassungsschutz und den Militärischen Abschirmdienst sowie die jeweilige Gesamtzahl ihrer Bediensteten anzugeben.

DRITTER ABSCHNITT

Übermittlungsvorschriften

§ 15

Zulässigkeit von Ersuchen

(1) Wird nach den Bestimmungen dieses Abschnittes um Übermittlung von personenbezogenen Daten ersucht, dürfen nur die Daten übermittelt werden, die bei der ersuchten Behörde bekannt sind oder aus allgemein zugänglichen Quellen entnommen werden können.

(2) Absatz 1 gilt nicht für besondere Ersuchen der Verfassungsschutzbehörden, des Militärischen Abschirmdienstes und des Bundesnachrichtendienstes um solche Daten, die bei der Wahrnehmung grenzpolizeilicher Aufgaben bekannt werden. Die Zulässigkeit dieser besonderen Ersuchen und ihre Erledigung regelt der Bundesminister des Innern in einer Dienstanweisung. Er unterrichtet die Parlamentarische Kontrollkommission über ihren Erlaß und erforderliche Änderungen. Satz 2 und 3 gilt nicht für die besonderen Ersuchen zwischen Behörden desselben Bundeslandes.

§ 16

Übermittlung von Informationen an die Verfassungsschutzbehörden

(1) Die Behörden des Bundes, der bundesunmittelbaren juristischen Personen des öffentlichen Rechts, die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie der Zoll, soweit er Aufgaben nach dem Bundesgrenzschutzgesetz wahrnimmt, unterrichten von sich aus das Bundesamt für Verfassungsschutz oder die Verfassungsschutzbehörde des Landes über die ihnen bekanntgewordenen Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht oder Bestrebungen im Geltungsbereich dieses Gesetzes erkennen lassen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1 und Nr. 3 genannten Schutzgüter gerichtet sind. Über Satz 1 hinausgehende Unterrichtungspflichten nach dem Gesetz über den Militärischen Abschirmdienst oder dem Gesetz über den Bundesnachrichtendienst bleiben unberührt. Auf die Übermittlung von Informationen zwischen Behörden desselben Bundeslandes findet Satz 1 keine Anwendung.

(2) Die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie der Zoll, soweit er Aufgaben nach dem Bundesgrenzschutzgesetz wahrnimmt, und der Bundesnachrichtendienst dürfen darüber hinaus von sich aus dem Bundesamt für Verfassungsschutz oder der Verfassungsschutzbehörde des Landes auch alle anderen ihnen bekanntgewordenen Informationen einschließlich personenbezogener Daten über Bestrebungen nach § 3 Abs. 1 übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist. Absatz 1 Satz 3 findet Anwendung.

(3) Das Bundesamt für Verfassungsschutz darf zur Erfüllung seiner Aufgaben die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie andere Behörden um Übermittlung der zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten ersuchen, wenn sie nicht aus allgemein zugänglichen Quellen oder nur mit übermäßigem Aufwand oder nur durch eine den Betroffenen stärker belastende Maßnahme erhoben werden

können. Unter den gleichen Voraussetzungen dürfen Verfassungsschutzbehörden der Länder

1. Behörden des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts,
2. Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, Polizeien des Bundes und anderer Länder um die Übermittlung solcher Informationen ersuchen.

(4) Würde durch die Übermittlung nach Absatz 3 Satz 1 der Zweck der Maßnahme gefährdet oder der Betroffene unverhältnismäßig beeinträchtigt, darf das Bundesamt für Verfassungsschutz amtliche Register einsehen.

(5) Die Ersuchen nach Absatz 3 sind aktenkundig zu machen. Über die Einsichtnahme nach Absatz 3 hat das Bundesamt für Verfassungsschutz einen Nachweis zu führen, aus dem der Zweck und die Veranlassung, die ersuchte Behörde und die Aktenfundstelle hervorgehen; die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten.

(6) Die Übermittlung personenbezogener Daten, die aufgrund einer Maßnahme nach § 100a der Strafprozeßordnung bekanntgeworden sind, ist nach den Vorschriften der Absätze 1, 2 und 3 nur zulässig, wenn tatsächliche Anhaltspunkte dafür bestehen, daß jemand eine der in § 2 des Gesetzes zu Artikel 10 Grundgesetz genannten Straftaten plant, begeht oder begangen hat. Auf die einer Verfassungsschutzbehörde nach Satz 1 übermittelten Kenntnisse und Unterlagen findet § 7 Abs. 3 und 4 des Gesetzes zu Artikel 10 Grundgesetz entsprechende Anwendung.

§ 17

**Übermittlung personenbezogener Daten
durch das Bundesamt für Verfassungsschutz**

(1) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an inländische Behörden übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt. Der Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

(2) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an Dienststellen der Stationierungsstreitkräfte im Rahmen von Artikel 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikvertrages über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Streitkräfte vom 3. August 1959 (BGBl. 1961 IIS. 1183) übermitteln. Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden und das Bundesamt für Verfassungsschutz sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

(3) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, wenn die Übermittlung zur Erfüllung seiner Aufgaben oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist. Die

Übermittlung unterbleibt, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Die Übermittlung ist aktenkundig zu machen. Der Empfänger ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden und das Bundesamt für Verfassungsschutz sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

(4) Personenbezogene Daten dürfen an andere Stellen nicht übermittelt werden, es sei denn, daß dies zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes erforderlich ist und der Bundesminister des Innern seine Zustimmung erteilt hat. Das Bundesamt für Verfassungsschutz führt über die Auskunft nach Satz 1 einen Nachweis, aus dem der Zweck der Übermittlung, ihre Veranlassung, die Aktenfundstelle und der Empfänger hervorgehen; die Nachweise sind gesondert aufzubewahren, gegen unberechtigten Zugriff zu sichern und am Ende des Kalenderjahres, das dem Jahr ihrer Erstellung folgt, zu vernichten. Der Empfänger darf die übermittelten Daten nur für den Zweck verwenden, zu dem sie ihm übermittelt wurden. Der Empfänger ist auf die Verwendungsbeschränkung und darauf hinzuweisen, daß das Bundesamt für Verfassungsschutz sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

§ 18

**Übermittlung von Informationen
durch das Bundesamt für Verfassungsschutz
an Strafverfolgungs- und Sicherheitsbehörden
in Angelegenheiten des Staats-
und Verfassungsschutzes**

(1) Das Bundesamt für Verfassungsschutz übermittelt den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien von sich aus die ihm bekanntgewordenen Informationen einschließlich personenbezogener Daten, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung zur Verhinderung oder Verfolgung von Staatsschutzdelikten erforderlich ist. Delikte nach Satz 1 sind die in §§ 74 a und 120 des Gerichtsverfassungsgesetzes genannten Straftaten sowie sonstige Straftaten, bei denen aufgrund ihrer Zielsetzung, des Motivs des Täters oder dessen Verbindung zu einer Organisation tatsächliche Anhaltspunkte dafür vorliegen, daß sie gegen die in Artikel 73 Nr. 10 Buchstabe b oder c des Grundgesetzes genannten Schutzgüter gerichtet sind. Das Bundesamt für Verfassungsschutz übermittelt dem Bundesnachrichtendienst von sich aus die ihm bekanntgewordenen Informationen einschließlich personenbezogener Daten, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der gesetzlichen Aufgaben des Empfängers erforderlich ist.

(2) Die Polizeien dürfen zur Verhinderung von Staatsschutzdelikten nach Absatz 1 Satz 2 das Bundesamt für Verfassungsschutz um Übermittlung der erforderlichen Informationen einschließlich personenbezogener Daten ersuchen. Der Bundesnachrichtendienst darf zur Erfüllung seiner Aufgaben das Bundesamt für Verfassungsschutz um die Übermittlung der erforderlichen Informationen einschließlich personenbezogener Daten ersuchen.

§ 19

Übermittlung von Informationen durch die Verfassungsschutzbehörden der Länder an Strafverfolgungs- und Sicherheitsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes

(1) Die Verfassungsschutzbehörden der Länder übermitteln den Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, den Polizeien Informationen einschließlich personenbezogener Daten unter den Voraussetzungen des § 18 Abs. 1 Satz 1 und 2 sowie Abs. 2 Satz 1. Auf die Übermittlung von Informationen zwischen Behörden desselben Bundeslandes findet Satz 1 keine Anwendung.

(2) Die Verfassungsschutzbehörden der Länder übermitteln dem Bundesnachrichtendienst und dem Militärischen Abschirmdienst Informationen einschließlich personenbezogener Daten unter den Voraussetzungen des § 18 Abs. 1 Satz 3 sowie Abs. 2 Satz 2.

§ 20

Übermittlung von Informationen durch die Staatsanwaltschaften und Polizeien an den Militärischen Abschirmdienst

Für die Übermittlung von Informationen einschließlich personenbezogener Daten durch die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie den Zoll, soweit er Aufgaben nach dem Bundesgrenzschutzgesetz wahrnimmt, an den Militärischen Abschirmdienst findet § 16 entsprechende Anwendung.

§ 21

Übermittlungsverbote

Die Übermittlung nach den Vorschriften dieses Abschnitts unterbleibt, wenn

1. für die übermittelnde Stelle erkennbar ist, daß unter Berücksichtigung der Art der Informationen und ihrer Erhebung die schutzwürdigen Interessen des Betroffenen das Allgemeininteresse an der Übermittlung überwiegen,
2. überwiegende Sicherheitsinteressen dies erfordern oder
3. besondere gesetzliche Übermittlungsregelungen entgegenstehen; die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

§ 22

Minderjährigenschutz

(1) Informationen einschließlich personenbezogener Daten über das Verhalten Minderjähriger dürfen nach den Vorschriften dieses Gesetzes übermittelt werden, solange die Voraussetzungen der Speicherung nach § 9. erfüllt sind. Liegen diese Voraussetzungen nicht mehr vor, bleibt eine Übermittlung nur zulässig, wenn sie zur Abwehr einer erheblichen Gefahr oder zur Verfolgung einer Straftat von erheblicher Bedeutung erforderlich ist.

(2) Informationen einschließlich personenbezogener Daten über das Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres dürfen nach den Vorschriften dieses Gesetzes nicht an ausländische oder über- oder zwischenstaatliche Stellen übermittelt werden.

§ 23

Pflichten des Empfängers

Der Empfänger prüft, ob die nach den Vorschriften dieses Gesetzes übermittelten personenbezogenen Daten für die Erfüllung seiner Aufgaben erforderlich sind. Ergibt die Prüfung, daß sie nicht erforderlich sind, hat er die Unterlagen zu vernichten. Die Vernichtung kann unterbleiben, wenn die Trennung von anderen Informationen, die zur Erfüllung der Aufgaben erforderlich sind, nicht oder nur mit unverhältnismäßigem Aufwand möglich ist; in diesem Fall sind die Daten zu sperren.

§ 24

Nachberichtspflicht

Erweisen sich personenbezogene Daten nach ihrer Übermittlung nach den Vorschriften dieses Gesetzes als unvollständig oder unrichtig, so sind sie unverzüglich gegenüber dem Empfänger zu berichtigen, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

§ 25

Automatisierte Abrufverfahren

Die Einrichtung eines automatisierten Verfahrens für Übermittlungen von personenbezogenen Daten nach §§ 16, 18, 19 und 20 ist nach Maßgabe des § 10 des Bundesdatenschutzgesetzes nur zulässig, wenn eine erhebliche Beeinträchtigung der freiheitlichen demokratischen Grundordnung droht oder eine konkrete Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes besteht und der für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesminister oder deren Vertreter der Einrichtung des Verfahrens zugestimmt haben. Die Einrichtung des Verfahrens ist zu befristen und der Abruf bei der speichernden Stelle aufzuzeichnen.

VIERTER ABSCHNITT

Schlußvorschriften

§ 26

Geltung des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 3 durch das Bundesamt für Verfassungsschutz finden die §§ 15 bis 20 des Bundesdatenschutzgesetzes in der Fassung des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes keine Anwendung.

§ 27

Berlin-Klausel

Dieses Gesetz gilt nach Maßgabe des § 13 Abs. 1 des Dritten Überleitungsgesetzes auch im Land Berlin.

Artikel 3

Gesetz über den Militärischen Abschirmdienst (MAD-Gesetz – MADG –)

§ 1

Aufgaben

(1) Der Militärische Abschirmdienst des Bundesministers der Verteidigung nimmt zur Sicherung der Einsatzbereitschaft der Streitkräfte nach Maßgabe dieses Gesetzes Aufgaben wahr, die denen einer Verfassungsschutzbehörde entsprechen.

(2) Aufgabe des Militärischen Abschirmdienstes ist die Sammlung und Auswertung von Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und Unterlagen, über

1. Bestrebungen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind,
2. sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht,

wenn sich diese Bestrebungen oder Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministers der Verteidigung richten und von Personen ausgehen oder ausgehen sollen, die diesem Geschäftsbereich angehören oder in ihm tätig sind. Bestrebungen gegen die freiheitlichdemokratische Grundordnung sind ziel- und zweckgerichtete Verhaltensweisen oder Betätigungen in der Regel in oder für Zwecke einer Organisation oder einer unorganisierten Gruppierung gegen dieses Schutzgut. Voraussetzung für die Sammlung und Auswertung von Informationen im Sinne des Satzes 1 ist das Vorliegen tatsächlicher Anhaltspunkte.

(3) Darüber hinaus obliegt dem Militärischen Abschirmdienst zur Beurteilung der Sicherheitslage

1. von Dienststellen und Einrichtungen im Geschäftsbereich des Bundesministers der Verteidigung und
2. von Dienststellen und Einrichtungen der verbündeten Streitkräfte und der internationalen militärischen Hauptquartiere, wenn die Bundesrepublik Deutschland in internationalen Vereinbarungen Verpflichtungen zur Sicherheit dieser Dienststellen und Einrichtungen übernommen hat und die Beurteilung der Sicherheitslage im Einvernehmen zwischen dem Bundesminister der Verteidigung und den zuständigen obersten Landesbehörden dem Militärischen Abschirmdienst übertragen worden ist,

die Auswertung von Informationen über die in Absatz 2 genannten Bestrebungen und Tätigkeiten gegen diese Dienststellen und Einrichtungen, auch soweit sie von Personen ausgehen oder ausgehen sollen, die nicht dem Geschäftsbereich des Bundesministers der Verteidigung angehören oder in ihm tätig sind.

(4) Der Militärische Abschirmdienst wirkt mit

1. bei der Sicherheitsüberprüfung von Personen, die dem Geschäftsbereich des Bundesministers der Verteidigung angehören, in ihm tätig sind oder werden sollen und
 - a) denen im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse anvertraut werden, die Zugang dazu erhalten sollen oder ihn sich verschaffen können, oder
 - b) die an sicherheitsempfindlichen Stellen des Geschäftsbereichs des Bundesministers der Verteidigung eingesetzt sind oder werden sollen,
2. bei technischen Sicherheitsmaßnahmen im Geschäftsbereich des Bundesministers der Verteidigung zum Schutz von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen gegen die Kenntniserhebung durch Unbefugte.

Besteht die Sicherheitsüberprüfung des Militärischen Abschirmdienstes nach Satz 1 lediglich in der Auswertung bereits vorhandenen Wissens der Beschäftigungsstelle, der Strafverfolgungs- oder Sicherheitsbehörden, ist es erforderlich und ausreichend, daß der Betroffene und die in die Sicherheitsüberprüfung einzubeziehenden Personen von der Einleitung der Überprüfung Kenntnis haben; im übrigen ist die Zustimmung erforderlich, soweit gesetzlich nichts anderes bestimmt ist. In die Sicherheitsüberprüfung dürfen der Ehegatte, Verlobte oder die Person, die mit dem Betroffenen in eheähnlicher Gemeinschaft lebt, miteinbezogen werden.

(5) Der Militärische Abschirmdienst darf einer polizeilichen Dienststelle nicht angegliedert werden.

(6) Der Militärische Abschirmdienst ist an die allgemeinen Rechtsvorschriften gebunden (Artikel 20 des Grundgesetzes).

§ 2

Zuständigkeit in besonderen Fällen

(1) Zur Fortführung von Aufgaben nach § 1 Abs. 2 kann der Militärische Abschirmdienst, soweit es im Einzelfall zwingend erforderlich ist, seine Befugnisse gegenüber Personen ausüben, die dem Geschäftsbereich des Bundesministers der Verteidigung nicht angehören oder nicht in ihm tätig sind. Dies ist nur zulässig

1. gegenüber dem Ehegatten oder Verlobten einer in § 1 Abs. 2 genannten Person oder dem mit ihr in eheähnlicher Gemeinschaft Lebenden, wenn angenommen werden muß, daß Bestrebungen oder Tätigkeiten nach § 1 Abs. 2 auch von ihm ausgehen,
2. im Benehmen mit der zuständigen Verfassungsschutzbehörde gegenüber Personen, bei denen tatsächliche Anhaltspunkte dafür bestehen, daß sie mit einer in § 1 Abs. 2 genannten Person bei Bestrebungen oder Tätigkeiten nach § 1 Abs. 2 zusammenarbeiten, und wenn anderenfalls die weitere Erforschung des Sachverhalts gefährdet oder nur mit übermäßigem Aufwand möglich wäre.

(2) Zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände und Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten kann der Militärische Abschirmdienst in Wahrnehmung seiner Aufgaben nach § 1 Abs. 2, soweit es im Einzelfall zwingend erforderlich ist, im Benehmen mit der zuständigen Verfassungsschutzbehörde seine Befugnisse gegenüber Personen ausüben, die dem Geschäftsbereich des Bundesministers der Verteidigung nicht angehören oder nicht in ihm tätig sind.

§ 3

Zusammenarbeit mit den Verfassungsschutzbehörden

(1) Der Militärische Abschirmdienst und die Verfassungsschutzbehörden arbeiten bei der Erfüllung ihrer Aufgaben zusammen. Die Zusammenarbeit besteht auch in gegenseitiger Unterstützung und Hilfeleistung.

(2) Zur Fortführung von Aufgaben nach § 3 Abs. 1 des Bundesverfassungsschutzgesetzes kann eine Ver-

fassungsschutzbehörde, soweit es im Einzelfall zwingend erforderlich ist, im Benehmen mit dem Militärischen Abschirmdienst Maßnahmen auf Personen erstrecken, die dem Geschäftsbereich des Bundesministers der Verteidigung angehören oder in ihm tätig sind und der Zuständigkeit des Militärischen Abschirmdienstes unterliegen. Dies ist nur zulässig gegenüber Personen, bei denen tatsächliche Anhaltspunkte dafür bestehen, daß sie mit einer Person aus dem Zuständigkeitsbereich der Verfassungsschutzbehörden bei Bestrebungen oder Tätigkeiten nach § 3 Abs. 1 des Bundesverfassungsschutzgesetzes zusammenarbeiten, und wenn anderenfalls die weitere Erforschung des Sachverhalts gefährdet oder nur mit übermäßigem Aufwand möglich wäre.

(3) Der Militärische Abschirmdienst und das Bundesamt für Verfassungsschutz unterrichten einander über alle Angelegenheiten, deren Kenntnis für die Erfüllung ihrer Aufgaben erforderlich ist.

§ 4

Befugnisse des Militärischen Abschirmdienstes

(1) Der Militärische Abschirmdienst darf die zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten erheben, verarbeiten und nutzen nach § 6 des Bundesverfassungsschutzgesetzes, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen in diesem Gesetz entgegenstehen. Er ist nicht befugt, personenbezogene Daten zur Erfüllung seiner Aufgaben nach § 1 Abs. 3 zu erheben. § 6 Abs. 2 Satz 2 und 3 des Bundesverfassungsschutzgesetzes findet Anwendung; die Zustimmung zur Dienstanweisung erteilt der Bundesminister der Verteidigung.

(2) Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Militärischen Abschirmdienst nicht zu; er darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen er selbst nicht befugt ist.

§ 5

Besondere Formen der Datenerhebung

Der Militärische Abschirmdienst darf Informationen, insbesondere personenbezogene Daten, nach § 7 des Bundesverfassungsschutzgesetzes erheben, soweit es

1. zur Erfüllung seiner Aufgaben nach § 1 Abs. 2 und § 2 Abs. 1 sowie zur Erforschung der dazu erforderlichen Quellen oder
2. zum Schutz der Mitarbeiter, Einrichtungen, Gegenstände und Quellen des Militärischen Abschirmdienstes gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten, auch nach § 2 Abs. 2,

erforderlich ist; § 7 Abs. 2 und 3 des Bundesverfassungsschutzgesetzes findet Anwendung.

§ 6

Speicherung, Veränderung und Nutzung personenbezogener Daten

(1) Der Militärische Abschirmdienst darf personenbezogene Daten nach § 8 des Bundesverfassungsschutzgesetzes speichern, verändern und nutzen, soweit es zur Erfüllung seiner Aufgaben erforderlich ist. Zur Erfüllung der Aufgaben nach § 1 Abs. 3 gespeicherte Daten über Personen, die nicht dem Geschäftsbereich des Bundesministers der Verteidigung angehören oder in ihm tätig sind, dürfen für andere Zwecke nicht verwendet werden, es sei denn, die Verwendung wäre auch für die Erfüllung der Aufgaben nach § 1 Abs. 2 zulässig.

(2) In Dateien gespeicherte Daten über Minderjährige sind nach zwei Jahren auf die Erforderlichkeit der Speicherung zu überprüfen und spätestens nach fünf Jahren zu löschen, es sei denn, daß nach Eintritt der Volljährigkeit weitere Erkenntnisse nach § 1 Abs. 2 oder § 2 angefallen sind. Dies gilt nicht, wenn der Betroffene nach § 1 Abs. 4 überprüft wird. Die Speicherung personenbezogener Daten über Minderjährige vor Vollendung des 16. Lebensjahres in zu ihrer Person geführten Akten und Dateien ist unzulässig.

§ 7

Berichtigung, Löschung und Sperrung personenbezogener Daten

(1) Der Militärische Abschirmdienst hat die in Dateien gespeicherten personenbezogenen Daten zu berichtigen, zu löschen und zu sperren nach § 40 des Bundesverfassungsschutzgesetzes.

(2) Der Militärische Abschirmdienst hat personenbezogene Daten in Akten zu berichtigen und zu sperren nach § 41 des Bundesverfassungsschutzgesetzes.

§ 8

Dateianordnungen

Der Militärische Abschirmdienst hat für jede automatisierte Datei mit personenbezogenen Daten eine Dateianordnung nach § 12 des Bundesverfassungsschutzgesetzes zu treffen, die der Zustimmung des Bundesministers der Verteidigung bedarf. § 12 Abs. 2 des Bundesverfassungsschutzgesetzes findet Anwendung.

§ 9

Auskunft an den Betroffenen

Der Militärische Abschirmdienst erteilt dem Betroffenen über zu seiner Person gespeicherte Daten Auskunft entsprechend § 13 des Bundesverfassungsschutzgesetzes; an die Stelle des dort genannten Bundesministers des Innern tritt der Bundesminister der Verteidigung.

§ 10

**Übermittlung von Informationen
an den Militärischen Abschirmdienst**

(1) Die Behörden des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts unterrichten von sich aus den Militärischen Abschirmdienst über die ihnen bekanntgewordenen Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht oder Bestrebungen im Geltungsbereich dieses Gesetzes erkennen lassen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 1 Abs. 2 Nr. 1 genannten Schutzgüter gerichtet sind, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die ~~Unterrichtung~~ zur Erfüllung seiner Aufgaben nach § 1 Abs. 2 und 3 erforderlich ist.

(2) Der Militärische Abschirmdienst darf nach § 16 Abs. 3 des Bundesverfassungsschutzgesetzes jede Behörde um die Übermittlung der zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten ersuchen.

(3) Würde durch die Übermittlung nach Absatz 2 der Zweck der Maßnahme gefährdet oder der Betroffene unverhältnismäßig beeinträchtigt, darf der Militärische Abschirmdienst amtliche Register einsehen. Diese Einsichtnahme bedarf der Zustimmung des Amtschefs des Amtes für den Militärischen Abschirmdienst oder seines Vertreters.

(4) § 15 Abs. 1 sowie § 16 Abs. 5 des Bundesverfassungsschutzgesetzes sind entsprechend anzuwenden.

§ 11

**Übermittlung personenbezogener Daten
durch den Militärischen Abschirmdienst**

(1) Der Militärische Abschirmdienst darf personenbezogene Daten nach § 17 Abs. 1 bis 3 des Bundesverfassungsschutzgesetzes übermitteln. Die Übermittlung an andere Stellen ist unzulässig.

(2) Der Militärische Abschirmdienst übermittelt Informationen einschließlich personenbezogener Daten an Staatsanwaltschaften, Polizeien und den Bundesnachrichtendienst nach § 18 des Bundesverfassungsschutzgesetzes.

§ 12

**Verfahrensregeln für die Übermittlung
von Informationen**

Für die Übermittlung von Informationen nach diesem Gesetz finden die §§ 24 bis 25 des Bundesverfassungsschutzgesetzes entsprechende Anwendung.

§ 13

Geltung des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 1 Abs. 2 bis 4 und § 2 finden die §§ 13 bis 20 des Bundesdatenschutzgesetzes in der Fassung des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes keine Anwendung.

Artikel 4

**Gesetz über den Bundesnachrichtendienst
(BND-Gesetz – BNDG –)**

§ 1

Organisation und Aufgaben

(1) Der Bundesnachrichtendienst ist eine Bundesoberbehörde im Geschäftsbereich des Chefs des Bundeskanzleramtes. Einer polizeilichen Dienststelle darf er nicht angegliedert werden.

(2) Der Bundesnachrichtendienst sammelt zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, die erforderlichen Informationen und wertet sie aus. Werden dafür im Geltungsbereich dieses Gesetzes Informationen einschließlich personenbezogener Daten erhoben, so richtet sich ihre Erhebung, Verarbeitung und Nutzung nach den §§ 2 bis 6 und 8 bis 11.

§ 2

Befugnisse

(1) Der Bundesnachrichtendienst darf die erforderlichen Informationen einschließlich personenbezogener Daten erheben, verarbeiten und nutzen, soweit nicht die anzuwendenden Bestimmungen des Bundesdatenschutzgesetzes oder besondere Regelungen in diesem Gesetz entgegenstehen.

1. zum Schutz seiner Mitarbeiter, Einrichtungen, Gegenstände und Quellen gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten,
2. für die Sicherheitsüberprüfung von Personen, die für ihn tätig sind oder tätig werden sollen,
3. für die Überprüfung der für die Aufgabenerfüllung notwendigen Nachrichtenzugänge und
4. über Vorgänge im Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, wenn sie nur auf diese Weise zu erlangen sind und für ihre Erhebung keine andere Behörde zuständig ist.

(2.) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist der Erhebungszweck anzugeben. Der Betroffene ist auf die Freiwilligkeit seiner Angaben und bei einer Sicherheitsüberprüfung nach Absatz 1 Nr. 2 auf eine dienst- und arbeitsrechtliche oder sonstige vertragliche Mitwirkungspflicht hinzuweisen.

Bei Sicherheitsüberprüfungen ist § 3 Abs. 3 Satz 2 und 3 des Bundesverfassungsschutzgesetzes entsprechend anzuwenden.

(3) Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Bundesnachrichtendienst nicht zu. Er darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen er selbst nicht befugt ist.

(4) Von mehreren geeigneten Maßnahmen hat der Bundesnachrichtendienst diejenige zu wählen, die den Betroffenen voraussichtlich am wenigsten beeinträchtigt. Eine Maßnahme darf keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zu dem beabsichtigten Erfolg steht.

§ 3

Besondere Formen der Datenerhebung

Der Bundesnachrichtendienst darf zur heimlichen Beschaffung von Informationen einschließlich perso-

nenbezogener Daten die Mittel gemäß § 6 Abs. 2. des Bundesverfassungsschutzgesetzes anwenden, wenn Tatsachen die Annahme rechtfertigen, daß dies zur Erfüllung seiner Aufgaben erforderlich ist. § 7 des Bundesverfassungsschutzgesetzes ist entsprechend anzuwenden.

§ 4

Speicherung, Veränderung und Nutzung personenbezogener Daten

(1) Der Bundesnachrichtendienst darf personenbezogene Daten nach § 8 des Bundesverfassungsschutzgesetzes speichern, verändern und nutzen, soweit es zur Erfüllung seiner Aufgaben erforderlich ist.

(2) Die Speicherung, Veränderung und Nutzung personenbezogener Daten über Minderjährige ist nur unter den Voraussetzungen des § 9 des Bundesverfassungsschutzgesetzes zulässig.

§ 5

Berichtigung, Löschung und Sperrung personenbezogener Daten

(1) Der Bundesnachrichtendienst hat die in Dateien gespeicherten personenbezogenen Daten zu berichtigen, zu löschen und zu sperren nach § 10 des Bundesverfassungsschutzgesetzes.

(2) Der Bundesnachrichtendienst hat personenbezogene Daten in Akten zu berichtigen und zu sperren nach § 11 des Bundesverfassungsschutzgesetzes.

§ 6

Datelanordnungen

Der Bundesnachrichtendienst hat für jede automatisierte Datei mit personenbezogenen Daten eine Datelanordnung nach § 12. des Bundesverfassungsschutzgesetzes zu treffen, die der Zustimmung des Chefs des Bundeskanzleramtes bedarf. § 12. Abs. 2 des Bundesverfassungsschutzgesetzes ist anzuwenden.

§ 7

Auskunft an den Betroffenen

Der Bundesnachrichtendienst erteilt dem Betroffenen auf Antrag Auskunft über zu seiner Person nach § 4. gespeicherte Daten entsprechend § 13. des Bundesverfassungsschutzgesetzes. An die Stelle des dort genannten Bundesministers des Innern tritt der Chef des Bundeskanzleramtes.

§ 8

**Übermittlung von Informationen
an den Bundesnachrichtendienst**

(1) Die Behörden des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts dürfen von sich aus dem Bundesnachrichtendienst die ihnen bekanntgewordenen Informationen einschließlich personenbezogener Daten übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für seine Eigensicherung nach § 2 Abs. 1 Nr. 1 erforderlich ist.

(2) Die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie der Zoll, soweit er Aufgaben nach dem Bundesgrenzschutzgesetz wahrnimmt, übermitteln dem Bundesnachrichtendienst von sich aus die ihnen bekanntgewordenen Informationen einschließlich personenbezogener Daten, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für seine Eigensicherung nach § 2 Abs. 1 Nr. 1 erforderlich ist.

(3) Der Bundesnachrichtendienst darf nach § 16 Abs. 2 des Bundesverfassungsschutzgesetzes jede Behörde um die Übermittlung der zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten ersuchen und nach § 16 Abs. 3 des Bundesverfassungsschutzgesetzes amtlich geführte Register einsehen, soweit es zur Erfüllung seiner Aufgaben erforderlich ist. § 1 Abs. 1 und § 16 Abs. 5 des Bundesverfassungsschutzgesetzes sind anzuwenden.

(4) Für die Übermittlung personenbezogener Daten, die aufgrund einer Maßnahme nach § 100a der Strafprozeßordnung bekanntgeworden sind, ist § 16 Abs. 6 des Bundesverfassungsschutzgesetzes entsprechend anzuwenden.

§ 9

**Übermittlung von Informationen
durch den Bundesnachrichtendienst**

(1) Der Bundesnachrichtendienst darf Informationen einschließlich personenbezogener Daten an inländische Behörden übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder wenn der Empfänger die Daten für Zwecke der öffentlichen Sicherheit benötigt. Der Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

(2) Für die Übermittlung von Informationen einschließlich personenbezogener Daten an andere Stellen ist § 17 Abs. 2 bis 4 des Bundesverfassungsschutzgesetzes entsprechend anzuwenden; dabei ist die Übermittlung nach Absatz 4 dieser Vorschrift nur zulässig, wenn sie zur Wahrung außen- und sicherheitspolitischer Belange der Bundesrepublik Deutschland erforderlich ist und der Chef des Bundeskanzleramtes seine Zustimmung erteilt hat.

(3) Der Bundesnachrichtendienst übermittelt Informationen einschließlich personenbezogener Daten an die Staatsanwaltschaften, die Polizeien und den Militärischen Abschirmdienst entsprechend § 18 des Bundesverfassungsschutzgesetzes.

§ 10

**Verfahrensregeln für die Übermittlung
von Informationen**

Für die Übermittlung von Informationen nach §§ 8 und 9 sind die §§ 21 bis 26 des Bundesverfassungsschutzgesetzes entsprechend anzuwenden.

§ 11

Geltung des Bundesdatenschutzgesetzes

Bei der Erfüllung der Aufgaben des Bundesnachrichtendienstes sind die §§ 13 bis 20 des Bundesdatenschutzgesetzes in der Fassung des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes nicht anzuwenden.

§ 12

Berichtspflicht

Der Bundesnachrichtendienst unterrichtet den Chef des Bundeskanzleramtes über seine Tätigkeit. Über die Erkenntnisse aus seiner Tätigkeit unterrichtet er darüber hinaus auch unmittelbar die Bundesminister im Rahmen ihrer Zuständigkeiten; hierbei ist auch die Übermittlung personenbezogener Daten zulässig.

§ 13

Berlin-Klausel

Dieses Gesetz gilt nach Maßgabe des § 13 Abs. 1 des Dritten Überleitungsgesetzes auch im Land Berlin.

Artikel 5

Berlin-Klausel

Dieses Gesetz gilt mit Ausnahme des Artikels 3 nach Maßgabe des § 13 Abs. 1 des Dritten Überleitungsgesetzes auch im Land Berlin.

Artikel 6

Inkrafttreten

(1) Dieses Gesetz tritt mit Ausnahme des Artikels 1 am Tage nach der Verkündung in Kraft; gleichzeitig tritt das Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes vom 27. September 1990 (BGBl. I S. 682), geändert durch das Gesetz vom 7. August 1992 (BGBl. I S. 1382), außer Kraft.

(2) Artikel 1 § 4 Abs. 4 Satz 3 tritt am ersten Tage des vierundzwanzigsten auf die Verkündung folgenden Kalendermonats in Kraft. Im übrigen tritt Artikel 1 am ersten Tage des sechsten auf die Verkündung folgenden Kalendermonats in Kraft; gleichzeitig treten das Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung vom 27. Januar 1977 (BGBl. I S. 201), die Datenschutzveröffentlichungsordnung vom 3. August 1977 (BGBl. I S. 1477), die Datenschutzgebührenordnung vom 22. Dezember 1977 (BGBl. I S. 3153) und die Datenschutzregisterordnung vom 9. Februar 1978 (BGBl. I S. 250) außer Kraft.

18.06.90

In - R

Berichtigung

zum

Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes

Deutscher Bundestag
Der Direktor

Bonn, den 18. Juni 1990

An den
Herrn Direktor des Bundesrates

Im Nachgang zu dem Schreiben der Präsidentin des Deutschen Bundestages vom 1. Juni 1990 teile ich mit, daß zu dem vom Deutschen Bundestag in seiner 214. Sitzung am 31. Mai 1990 beschlossenen Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes - Drucksachen 11/4306, 11/7235 - folgende Berichtigungen erforderlich sind:

1. In § 11 Abs. 1 Satz 2 sind die Worte "§§ 6 und 7" durch die Worte "§§ 6 bis 8" zu ersetzen.
2. In § 12 trägt der letzte Absatz die Nummer 4.
3. In § 17 Abs. 1 sind die Worte "§ 14 Abs. 1" durch die Worte "§ 16 Abs. 1" zu ersetzen.
4. In § 24 endet der Absatz 1 nach den Worten "auf den Einzelfall beschränkt". Die mit den Worten "auftragten hinreichende Anhaltspunkte" beginnende anschließende Wiederholung entfällt.

- 2 -

5. In § 26 Abs. 5 lautet der 5. Satz wie folgt:
"Die Angaben nach § 18 Abs. 2 Satz 2 Nr. 3 und 5 über Dateien der in § 6 Abs. 2 genannten Behörden unterliegen nicht der Einsichtnahme."
6. § 30 Abs. 4 lautet wie folgt:
"(4) Die §§ 29, 33 bis 35 gelten nicht."
7. In § 44 Abs. 1 Nr. 1 werden die Worte "§ 29 Abs. 2 Satz 2 oder 3" ersetzt durch die Worte "§ 29 Abs. 2 Satz 3 oder 4".
8. In Artikel 2 § 16 Abs. 5 sind in Satz 2 die Worte "nach Absatz 3" durch die Worte "nach Absatz 4" zu ersetzen.
9. In Artikel 2 § 26 sind die Worte "§§ 15 bis 20" zu ersetzen durch "§§ 13 bis 20".
10. Artikel 4 § 8 Abs. 3 lautet wie folgt:
"(3) Der Bundesnachrichtendienst darf nach § 16 Abs. 3 des Bundesverfassungsschutzgesetzes jede Behörde um die Übermittlung der zur Erfüllung seiner Aufgaben erforderlichen Informationen einschließlich personenbezogener Daten ersuchen und nach § 16 Abs. 4 des Bundesverfassungsschutzgesetzes amtlich geführte Register einsehen, soweit es zur Erfüllung seiner Aufgaben erforderlich ist. § 15 Abs. 1 und § 16 Abs. 5 des Bundesverfassungsschutzgesetzes sind anzuwenden."



(Dr. Blicher)

22.06.90

Anrufung des Vermittlungsausschusses

durch den Bundesrat

zum

Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes

Der Bundesrat hat in seiner 615. Sitzung am 22. Juni 1990 beschlossen, zu dem Gesetz die Einberufung des Vermittlungsausschusses gemäß Artikel 77 Abs. 2 des Grundgesetzes aus folgenden Gründen zu verlangen:

1. Zu Artikel 1 (§ 1 BDSG)

In Artikel 1 ist § 1 wie folgt zu fassen:

"§ 1

Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(noch Ziffer 1)

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
 - a) Bundesrecht ausführen oder
 - b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,

3. nicht-öffentliche Stellen.

(3) Für automatisierte Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend erstellt und nach ihrer verarbeitungstechnischen Nutzung automatisch gelöscht werden, gelten nur die §§ 5 und 9.

(4) Dieses Gesetz gilt nicht

1. für natürliche Personen, die personenbezogene Daten ausschließlich für private Zwecke und zum persönlichen Gebrauch verarbeiten oder nutzen,
2. a) für öffentlich-rechtliche Religionsgesellschaften sowie die ihnen zugeordneten caritativen und erzieherischen Einrichtungen des öffentlichen Rechts,
 - b) mit Ausnahme der §§ 8, 28, 29, 33 bis 35 für die den öffentlich-rechtlichen Religionsgesellschaften zugeordneten caritativen und erzieherischen Einrichtungen des privaten Rechts.

(noch Ziffer 1)

(5) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(6) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden."

Begründung:

Zu § 1 Abs. 2 Nr. 3, zum Wegfall von § 1 Abs. 3 des Gesetzesbeschlusses, zu § 1 Abs. 4:

Die in Absatz 3 des Gesetzesbeschlusses vorgesehene Neuregelung der Anwendbarkeit des BDSG im nicht-öffentlichen Bereich ist zumindest tendenziell auf erhebliche, sachlich nicht vertretbare Einschränkungen des Geltungsbereichs des Gesetzes angelegt. So würde bei einer restriktiven Interpretation des Wortes "geschäftsmäßig" die Verarbeitung personenbezogener Daten beispielsweise durch Vereine, Parteien und Gewerkschaften nicht mehr unter den Schutz dieses Gesetzes fallen. Demgegenüber ist nach Absatz 4 Nr. 1 des Regierungsentwurfs, der hier als neuer Absatz 4 übernommen wird, lediglich die Verarbeitung personenbezogener Daten aus dem Anwendungsbereich des Gesetzes herausgenommen, die ausschließlich für private Zwecke und zum persönlichen Gebrauch erfolgt. Schon aus Gründen der Rechtsklarheit sollte es deshalb hinsichtlich der Absätze 2 und 4 bei der Fassung des Regierungsentwurfs verbleiben mit der Maßgabe, daß auch für den nicht-öffentlichen Bereich die Erhebung in den Anwendungsbereich des Gesetzes einbezogen wird.

(noch Ziffer 1)

Zu Absatz 3:

Für die prinzipielle Unterscheidung zwischen sog. externen und sog. internen Dateien ist ein sachlich überzeugender Grund nicht mehr ersichtlich, zumal nunmehr auch die aktenmäßige Datenverarbeitung jedenfalls durch öffentliche Stellen in den Anwendungsbereich des Gesetzes einbezogen wird.

Zu Absatz 6:

Wegen der prinzipiellen Gleichrangigkeit des Verwaltungsverfahrensgesetzes und des Bundesdatenschutzgesetzes für die öffentlich-rechtliche Verwaltungstätigkeit bedarf es der Klärung, in welchem Verhältnis diese beiden Gesetze zueinander stehen. Mit der vorgeschlagenen Regelung wird klargestellt, daß das Datenschutzgesetz Vorrang hat, soweit es um die Ermittlung des Sachverhalts geht; die diesbezüglichen Regelungen des Verwaltungsverfahrensgesetzes sollen künftig insoweit nur eingeschränkt Anwendung finden. Im übrigen wird davon ausgegangen, daß die Regelungen beider Gesetze nebeneinander gelten und sich zum Teil ergänzen, soweit nicht das Verwaltungsverfahrensgesetz eine speziellere, vom Bundesdatenschutzgesetz abweichende Regelung enthält.

2. Zu Artikel 1 (§ 10 BDSG)

In Artikel 1 ist in § 10 der Absatz 3 wie folgt zu fassen:

"(3) Im Bereich der öffentlichen Stellen des Bundes darf ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte nur eingerichtet werden, wenn eine Rechtsvorschrift dies zuläßt. Die Bundesminister werden ermächtigt, nach Maßgabe der Absätze 1 und 2 automatisierte Abrufverfahren für ihren Geschäftsbereich durch Rechtsverordnung einzuführen. Der Bundesbeauftragte für den Datenschutz ist über die beabsichtigte Regelung zu unterrichten.

Begründung:

Die unter Gesichtspunkten des Datenschutzes besonders bedeutsame Einrichtung automatisierter Abrufverfahren sollte - entsprechend dem Beschluß des Bundesrates vom 10. Februar 1989 (BR-Drs. 618/88 (Beschluß), A Nr. 15) - im öffentlichen Bereich grundsätzlich nur nach Maßgabe einer speziellen Rechtsvorschrift zugelassen werden.

3. Zu Artikel 1 (§ 14 BDSG)

In Artikel 1 ist in § 14 der Absatz 2 wie folgt zu ändern:

a) In Satz 1 Nr. 3 ist nach den Worten

"Betroffenen liegt"

ein Komma einzufügen.

b) Satz 1 Nr. 4 sowie die Sätze 2 und 3 sind zu streichen.

c) In Satz 1 ist Nummer 7 wie folgt zu fassen:

"7. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder unmittelbar drohender Gefahren für Leib, Leben oder persönliche Freiheit anderer erforderlich ist,".

d) In Satz 1 ist Nummer 9 zu streichen.

e) In Satz 1 ist Nummer 10 wie folgt zu fassen:

"10. es zur Durchführung eines bestimmten Forschungsvorhabens erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann."

(noch Ziffer 3)

Begründung:

zu a:

Klarstellung, daß sich die Offensichtlichkeit nur auf das Vorliegen des Interesses des Betroffenen beziehen soll.

zu b:

Die bisher in Nummer 4 vorgesehene Regelung würde eine Umgehung des gesetzgeberischen Willens in allen Fällen ermöglichen, in denen für bestimmte Zwecke (z.B. Statistiken) ein besonderes Erhebungsverfahren vorgesehen ist. Als Folge müssen dann auch die Sätze 2 und 3 entfallen.

zu c und d:

Die Änderungen dienen der Zielsetzung, den Ausnahmekatalog auf das Notwendige zu beschränken.

zu e:

Bei sachgerechter Abwägung zwischen dem Grundrecht auf informationelle Selbstbestimmung und der Forschungsfreiheit kann letzter der Vorrang nur dann zugesprochen werden, wenn die Datenverarbeitung für ein bestimmtes Forschungsvorhaben erfolgt und dieses Vorhaben ohne die zweckfremde Datenverarbeitung nicht oder nur unter unverhältnismäßigen Schwierigkeiten durchgeführt werden kann. An dieser Voraussetzung fehlt es z.B., wenn das Vorhaben auch mit anonymisierten Daten durchgeführt werden kann.

4. Zu Artikel 1 (§ 15 BDSG)

In Artikel 1 ist in § 15 folgender Absatz 6 anzufügen:

"(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden."

Begründung:

Die Weitergabe von Daten innerhalb einer öffentlichen Stelle ist keine Übermittlung im Sinne des § 15. Der in Absatz 5 zum Ausdruck gekommene Gedanke der Verwaltungsvereinfachung gilt erst recht für die Weitergabe innerhalb einer öffentlichen Stelle.

5. Zu Artikel 1 (§ 16 BDSG)

In Artikel 1 ist in § 16 Abs. 1 die Nummer 2 wie folgt zu fassen:

"2. es zur Wahrung berechtigter Interessen, die der Empfänger glaubhaft dargelegt hat, erforderlich ist und schutzwürdige Interessen des Betroffenen nicht entgegenstehen."

Begründung:

Der Erforderlichkeitsgrundsatz gilt auch für die Datenübermittlung an nicht-öffentliche Stellen; das bedarf der ausdrücklichen Verdeutlichung (vgl. auch die Formulierung in § 28 Abs. 2 Nr. 1 Buchstabe d).

6. Zu Artikel 1 (§ 17 BDSG)

In Artikel 1 sind in § 17 die Absätze 1 und 2 wie folgt zu fassen:

"(1) Eine Übermittlung personenbezogener Daten an ausländische, an über- oder zwischenstaatliche Stellen oder an Stellen der Deutschen Demokratischen Republik ist zulässig, soweit die Übermittlung in einem Gesetz, einem Rechtsakt der Europäischen Gemeinschaften oder einer internationalen Vereinbarung ausdrücklich geregelt ist.

(2) Eine Übermittlung darf auch erfolgen, wenn für den Empfänger gleichwertige Datenschutzregelungen gelten und bei einer Übermittlung an öffentliche Stellen die Voraussetzungen des § 15 Abs. 1, im Übrigen die Voraussetzungen des § 16 Abs. 1 und 3 erfüllt sind. Die Übermittlung unterbleibt, soweit Grund zu der Annahme besteht, daß sie gegen den Zweck eines deutschen Gesetzes, insbesondere gegen § 1 Abs. 1, verstoßen würde."

Begründung:

Die Fassung des Gesetzesbeschlusses beläßt das Verhältnis zwischen einer zulässigen Übermittlung nach BDSG und einer zulässigen Übermittlung nach bereichsspezifischen Vorschriften im Unklaren.

Die Neufassung verdeutlicht, daß eine Übermittlung an ausländische Stellen in zwei Alternativen zulässig ist: Entweder sind die Voraussetzungen in einer bereichsspezifischen Vorschrift festgelegt (Absatz 1) oder die Zulässigkeit bestimmt sich nach den Kriterien des BDSG für eine Übermittlung im öffentlichen bzw. im nicht-öffentlichen Bereich, sofern die Gleichwertigkeit des Datenschutzes auch im Ausland sichergestellt ist (Absatz 2).

379/90

7. Zu Artikel 1 (§ 24 BDSG)

In Artikel 1 ist § 24 wie folgt zu ändern:

- a) In Absatz 1 Satz 1 sind die Worte
", unbeschadet der ihnen bei der Erfüllung ihrer
Aufgaben obliegenden fachlichen Beurteilung und
Verantwortlichkeit,"
zu streichen.
- b) In Absatz 1 ist der Satz 2 zu streichen.
- c) In Absatz 2 sind die Sätze 3 und 4 durch folgende
Sätze 3 bis 5 zu ersetzen:

"Das Kontrollrecht erstreckt sich nicht auf den Inhalt des Post- und Fernmeldeverkehrs, soweit sich nicht aus Satz 4 etwas anderes ergibt. Die Kontrolle des Bundesbeauftragten für den Datenschutz erstreckt sich auf personenbezogene Daten, die der Kontrolle durch die Kommission nach § 9 des Gesetzes zu Artikel 10 GG unterliegen, insoweit, als die Kommission diesen ersucht, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren. Über das Ergebnis ist nur der Kommission zu berichten."

Begründung:

zu a):

Die Kompetenzen des Bundesbeauftragten für den Datenschutz werden in diesem Gesetz eindeutig geregelt. Der Hinweis auf die Verantwortlichkeit der datenverarbeitenden Stellen in fachlicher Hinsicht ist daher eher geeignet, zu Fehlinterpretationen Anlaß zu geben.

(noch Ziffer 7)

zu b und c:

Durch die vorgeschlagenen Änderungen wird eine prinzipiell uneingeschränkte, auch systematische Kontrolle durch den Bundesbeauftragten für den Datenschutz in allen Verwaltungsbereichen, ohne Rücksicht auf die Art der dabei in Betracht zu ziehenden personenbezogenen Daten und die jeweilige Form der Datenverarbeitung, wie sie bereits im wesentlichen auch der bisherigen Kontrollpraxis entspricht, ausdrücklich legitimiert.

Durch die - beizubehaltende - Verweisung in Absatz 6 auf Absatz 2 in der vorgeschlagenen geänderten Fassung wird eine entsprechende Klarstellung für die Datenschutzkontrolle in den Ländern erreicht. Die in der vorliegenden Gesetzesfassung auch für die Datenschutzkontrolle in den Ländern vorgesehenen erheblichen Einschränkungen der Kontrollbefugnisse sind mit den Zielsetzungen der neuen Landesdatenschutzgesetze nicht zu vereinbaren. Sie entsprechen auch nicht der bisherigen Kontrollpraxis in den Ländern und sind sachlich nicht geboten.

8. Zu Artikel 1 (§ 27 BDSG)

In Artikel 1 ist § 27 wie folgt zu ändern:

- a) In Absatz 1 Satz 1 ist der einleitende Teilsatz wie folgt zu fassen:

"Die Vorschriften dieses Abschnittes gelten für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch".

- b) In Absatz 2
ist das Wort "offensichtlich"
zu streichen.

Begründung:

zu a:

Auch für nicht-öffentliche Stellen muß die Zulässigkeit der Erhebung geregelt werden. Dies folgt aus dem Recht auf informationelle Selbstbestimmung und Artikel 5a der Datenschutzkonvention des Europarates.

Der Bundesrat hat bereits in seiner Stellungnahme vom 10.2.1989 (BR-Drs. 618/88 (Beschluss), A Ziff. 1) die Schaffung angemessener Schutzvorschriften für die Datenerhebung vorgeschlagen.

zu b:

Entscheidend ist, daß Daten in Akten aus einer Datei entnommen worden sind. Die Beschränkung auf eine "offensichtliche" Entnahme würde auch zu Abgrenzungsschwierigkeiten führen, für die das Gesetz keinen Maßstab liefert.

9. Zu Artikel 1 (§ 28 BDSG)

In Artikel 1 ist § 28 wie folgt zu ändern:

a) In Absatz 1 Satz 1 ist
eingangs vor dem Wort "Speichern"
das Wort "Erheben,"
einzufügen.

b) In Absatz 1 ist Nummer 4, wie folgt zu fassen:

"4. wenn es im Interesse der speichernden Stelle zur Durchführung eines bestimmten Forschungsvorhabens erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann."

c) In Absatz 2 ist Nummer 3 wie folgt zu fassen:

"3. wenn es im Interesse einer Forschungseinrichtung zur Durchführung eines bestimmten Forschungsvorhabens erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluß der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann."

d) In Absatz 4 ist Satz 1 wie folgt zu fassen:

"Der Empfänger darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden."

(noch Ziffer 9)

Begründung:

zu a:

Zur Notwendigkeit der Erfassung der Erhebungsphase im nicht-öffentlichen Bereich siehe die Änderungsvorschläge zu § 1 und zu § 27. Ferner wird auf § 30 Abs. 1 Satz 1 des Entwurfs der SPD-Fraktion im Deutschen Bundestag für ein Bundes-Informationsschutzgesetz, BT-Drs. 11/3730, verwiesen.

zu b und c:

Siehe den Änderungsvorschlag zu § 14 Abs. 2 Nr. 10 (Forschungsklausel).

zu d:

Für eine Beschränkung der Zweckbindung beim Empfänger auf den Fall, daß die Übermittlung zur Wahrung berechtigter Interessen eines Dritten (Absatz 2 Nr. 1 Buchstabe a) erfolgt, ist eine Rechtfertigung nicht ersichtlich. Der Umfang der Zweckbindung beim Empfänger darf in keinem der Übermittlungsfälle geringer sein als bei der übermittelnden Stelle selbst. Vgl. zur Zweckbindung im übrigen Artikel 5b und 5c der Datenschutzkonvention des Europarates.

10. Zu Artikel 1 (§ 29 BDSG)

In Artikel 1 ist § 29 wie folgt zu ändern:

a) In Absatz 1 Satz 1 ist
eingangs vor dem Wort "Speichern"
das Wort "Erheben,"
einzufügen.

b) Absatz 3 ist wie folgt zu fassen:

"(3) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 3 und 4."

Begründung:

zu a:

Siehe die Änderungsvorschläge zu den §§ 1, 27 und 28.
Weiter wird auf § 40 Abs. 1 Satz 1 des Entwurfs der
SPD-Fraktion im Deutschen Bundestag für ein Bundes-Infor-
mationsschutzgesetz, BT-Drs. 11/3730, verwiesen.

zu b:

Für eine Freistellung der Übermittlung für Zwecke der
Werbung oder der Markt- und Meinungsforschung von den
Widerspruchsrechten nach § 28 Abs. 3 und der Zweckbin-
dung nach § 28 Abs. 4 ist ein zwingender Grund nicht er-
kennbar.

11. Zu Artikel 1 (§ 29a - neu - BDSG)

In Artikel 1 ist nach § 29 folgender § 29a einzufügen:

"§ 29a

Datenübermittlung an Stellen außerhalb des
Geltungsbereichs dieses Gesetzes

(1) Die Übermittlung an Stellen außerhalb des Geltungsbereichs dieses Gesetzes ist zulässig, wenn die Voraussetzungen der §§ 28 oder 29 erfüllt sind und für den Empfänger gleichwertige Datenschutzregelungen gelten.

(2) Soweit im Empfängerland keine gleichwertigen gesetzlichen Datenschutzregelungen gelten, ist der Betroffene über die Übermittlung, den Empfänger und die Datenschutzrechte und -pflichten zu unterrichten, die der Empfänger im Interesse des Betroffenen zu beachten hat.

(3) Im übrigen gilt § 17 Abs. 3 und 4."

Begründung:

Auch für nicht-öffentliche Stellen bedarf es einer Regelung über die Zulässigkeit grenzüberschreitender Datenübermittlungen. Dies gilt insbesondere angesichts der bevorstehenden Vollendung des Europäischen Binnenmarktes. Für den Empfänger müssen Datenschutzregelungen gelten, die denen im Inland vergleichbar sind, weil der Betroffene hinsichtlich seiner ins Ausland übermittelten Daten vom deutschen Gesetzgeber nicht schutzlos gestellt werden darf. Anderenfalls wäre sein Persönlichkeitsrecht mangels Schutzvorkehrungen schwerwiegend gefährdet (so ausdrücklich Art. 4 Abs. 2 des Entwurfs für ein Datenschutzgesetz der Schweiz von 1988).

(noch Ziffer 11)

Soweit im Ausland gesetzliche Regelungen fehlen, die einen gleichwertigen Datenschutz gewährleisten, kommen bei fehlender Beteiligung des Betroffenen vertragliche Regelungen zu seinen Gunsten nach § 328 BGB in Betracht, die ihm einklagbare Rechte geben.

Absatz 2 gibt dem Betroffenen die Möglichkeit, Beeinträchtigungen seines Persönlichkeitsrechts im Ausland festzustellen und abzuwehren.

Vergleiche im übrigen den Änderungsvorschlag zu § 17.

12. Zu Artikel 1 (§ 33 BDSG)

In Artikel 1 ist in § 33 der Absatz 1 wie folgt zu fassen:

"(1) Werden erstmals personenbezogene Daten gespeichert, ist der Betroffene über die Speicherung und die Art der Daten zu benachrichtigen."

Begründung:

Auch bei geschäftsmäßiger Speicherung zum Zwecke der Übermittlung ist eine Benachrichtigung des Betroffenen über die erstmalige Speicherung - nicht erst über die erstmalige Übermittlung - erforderlich, damit er über sein Auskunftsrecht schon vor der Übermittlung die Richtigkeit der zu seiner Person gespeicherten Daten prüfen kann. Auskunftsteile und Detekteien haben ihre Informationen zu allermeist nicht vom Betroffenen selbst, so daß Anlaß besteht, ihm schon zu Beginn der Datenverarbeitung die Möglichkeit zu geben, von seinem Recht auf informationelle Selbstbestimmung Gebrauch zu machen.

Vergleiche im übrigen den gleichen Änderungsvorschlag des Bundesrates in seinem Beschluß vom 10.2.1989 (BR-Drs. 618/88 (Beschluß), A Ziff. 38).

13. Zu Artikel 1 (§§ 38 und 44 BDSG)

In Artikel 1 sind die §§ 38 und 44 wie folgt zu ändern:

- a) In § 38 Abs. 5 ist Satz 1 durch folgende Sätze zu ersetzen:

"Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, soweit diese die Verarbeitung oder Nutzung personenbezogener Daten in oder aus Dateien regeln, kann die Aufsichtsbehörde bei schwerwiegenden Datenschutzverstößen die Erhebung, Verarbeitung und Nutzung personenbezogener Daten untersagen und die Löschung gespeicherter Daten anordnen. Sie kann ferner anordnen, daß im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden."

- b) In § 44 Abs. 1 ist Nummer 7 wie folgt zu fassen:

"7. einer vollziehbaren Maßnahme nach § 38 Abs. 5 Sätze 1 bis 3."

Begründung:

zu a):

Eine ähnliche Regelung enthält § 38 Abs. 5 Satz 1 Nr. 3 des Entwurfs der SPD-Fraktion im Deutschen Bundestag eines Bundes-Informationsschutzgesetzes, BT-Drs. 11/3730. Auch ist auf ausländische Vorbilder zu verweisen.

Die Untersagung materieller Datenschutzverstöße außerhalb der Datensicherung soll lediglich als letztes Mittel in Betracht kommen, wenn sich die nicht-öffentliche Stelle auch nach eingehender Belehrung und Beratung

(noch Ziffer 13)

durch die Aufsichtsbehörde nicht zum Einlenken bereit zeigt. Eine Untersagung ist etwa im Hinblick auf Warndateien in Betracht zu ziehen, in denen ungesicherte Informationen sensibler Art gespeichert werden, ohne daß sich die Betroffenen dagegen - oft schon mangels Kenntnis von der Speicherung bestimmter Daten - wirksam zur Wehr setzen können.

Das Klagerisiko muß in solchen Fällen beim Betreiber der Datei liegen (Anfechtung der Untersagungsverfügung). Die Untersagung durch die Aufsichtsbehörde ermöglicht einen frühzeitigen und effektiven Schutz der Gesamtheit der Betroffenen.

Die bloße Existenz einer derartigen Untersagungsmöglichkeit wird die Position der obersten Aufsichtsbehörden für den Datenschutz in ihren Gesprächen mit den Spitzenverbänden der Wirtschaft erheblich stärken.

zu b:

Bei § 38 Abs. 5 sollten nicht nur Maßnahmen nach Satz 1, sondern auch nach den Sätzen 2 und 3 bußgeldbewehrt sein.

14. Zu Artikel 1 (§ 40)

In Artikel 1 ist in § 40 folgender Absatz 5 anzufügen:

"(5) Die wissenschaftliche Forschung betreibende Stelle hat dafür zu sorgen, daß die Verarbeitung oder Nutzung der Daten räumlich und organisatorisch getrennt von der Erfüllung anderer als wissenschaftlicher Aufgaben erfolgt."

Begründung:

Übernahme der Regelung in § 36 Abs. 9 Satz 2 des Regierungsentwurfs. Jede Forschungseinrichtung muß durch organisatorische und verfahrensmäßige Vorkehrungen sicherstellen, daß die personenbezogenen Daten nur für den Forschungszweck verwendet werden.

15. Zu Artikel 1 (§ 41 BDSG)

In Artikel 1 sind in § 41 Abs. 1 Satz 2 die Worte "journalistisch-redaktionelle" durch die Worte "meinungsbildende journalistisch-redaktionelle" zu ersetzen.

Begründung:

Die Änderung entspricht dem Wortlaut des Regierungsentwurfs. Für Adressen- Telefon- Branchen- oder vergleichbare Verzeichnisse, wie etwa Schuldnerlisten, Konkurs- und Zwangsversteigerungskataloge, besteht keine Rechtfertigung, das Presseprivileg zu gewähren und einen Schutz gegen Datenschutzverstöße zu versagen. Eigentlicher Zweck dieser Verzeichnisse, die oft sensitive Daten enthalten, ist die Datenübermittlung. Die Beifügung redaktioneller Texte darf nicht zur Umgehung des Datenschutzes führen.

16. Zu Artikel 1 (§ 43 BDSG)

In Artikel 1 ist § 43 wie folgt zu ändern:

- a) In Absatz 1 sind die Eingangsworte wie folgt zu fassen:

"Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,"

- b) In Absatz 1 Nr. 3
sind die Worte "aus Dateien"
zu streichen.

- c) In Absatz 2 ist Nummer 1 wie folgt zu fassen:

"1. die Übermittlung von durch dieses Gesetz geschützten Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht,".

- d) In Absatz 2 Nr. 2
sind nach den Worten "§ 29 Abs. 3, oder"
die Worte "entgegen § 39 oder"
einzufügen.

Begründung:

zu a):

Vergleiche die Einleitung zu § 41 Abs. 1 des geltenden Gesetzes. In § 1 Abs. 2 und 3 in der Fassung des Gesetzesbeschlusses werden keine "Voraussetzungen für personenbezogene Daten" aufgestellt.

(noch Ziffer 16)

zu b:

Die Beschränkung auf Dateien ist angesichts der Erweiterung auf Akten im öffentlichen Bereich nicht einsichtig.

zu c:

Vergleiche die Begründung zu a.

zu d:

Gerade bei Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen (siehe § 39), ist ein strafrechtlicher Schutz hinsichtlich unbefugter Zweckänderung erforderlich.

17. Zu Artikel 2 (§ 1 BVerfSchG)

In Artikel 2 ist in § 1 Abs. 1 nach den Worten
"der Länder"
die Worte
"und der Abwehr der diesen Schutzgütern drohenden
Gefahren"
einzufügen.

Begründung:

Klarstellung der Gefahrenabwehrfunktion der Verfassungsschutzbehörden (wie auch in § 1 des Gesetzes zu Artikel 10 GG).

18. Zu Artikel 2 (§ 1 BVerfSchG)

In Artikel 2 ist in § 1 der Absatz 3 zu streichen.

Begründung:

Die klare Regelung des Absatzes 2 reicht aus, die Verpflichtung zur Zusammenarbeit zu normieren. Absatz 3 ist daher entbehrlich. Überdies besteht die Gefahr, daß eine klare Zuständigkeitsabgrenzung verwischt wird (vgl. auch den Änderungsvorschlag für einen neuen § 3b).

19. Zu Artikel 2 (§ 3 und § 3a - neu - BVerfSchG)

Artikel 2 ist wie folgt zu ändern:

- a) In § 3 ist der Absatz 2 zu streichen.
- b) Nach § 3 ist folgender § 3a einzufügen:

"§ 3a

Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes sind

- a) Bestrebungen gegen den Bestand des Bundes oder eines Landes solche politisch motivierten ziel- und zweckgerichteten Verhaltensweisen in oder für einen Personenzusammenschluß, der darauf gerichtet ist, die Freiheit des Bundes oder eines Landes von fremder Herrschaft aufzuheben, ihre staatliche Einheit zu beseitigen oder ein zu ihnen gehörendes Gebiet abzutrennen;
- b) Bestrebungen gegen die Sicherheit des Bundes oder eines Landes solche politisch motivierten ziel- und zweckgerichteten Verhaltensweisen in oder für einen Personenzusammenschluß, der darauf gerichtet ist, den Bund, Länder oder deren Einrichtungen in ihrer Funktionsfähigkeit erheblich zu beeinträchtigen;

(noch Ziffer 19)

- c) Bestrebungen gegen die freiheitliche demokratische Grundordnung solche politisch motivierten ziel- und zweckgerichteten Verhaltensweisen in oder für einen Personenzusammenschluß, der darauf gerichtet ist, einen der in Absatz 2 genannten Verfassungsgrundsätze zu beseitigen oder außer Geltung zu setzen.

Für einen Personenzusammenschluß handelt, wer ihn in nicht unmaßgeblicher Weise in seinen Bestrebungen unterstützt. Verhaltensweisen von Einzelpersonen, die nicht in oder für einen Personenzusammenschluß handeln, sind Bestrebungen im Sinne dieses Gesetzes, wenn sie auf Anwendung von Gewalt gerichtet sind oder aufgrund ihrer Wirkungsweise geeignet sind, ein Schutzgut dieses Gesetzes erheblich zu beschädigen.

(2) Zur freiheitlichen demokratischen Grundordnung im Sinne dieses Gesetzes zählen:

- a) das Recht des Volkes, die Staatsgewalt in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung auszuüben und die Volksvertretung in allgemeiner unmittelbarer, freier, gleicher und geheimer Wahl zu wählen,
- b) die Bindung der Gesetzgebung an die verfassungsmäßige Ordnung und die Bindung der vollziehenden Gewalt und der Rechtsprechung an Gesetz und Recht,
- c) das Recht auf Bildung und Ausübung einer parlamentarischen Opposition,
- d) die Ablösbarkeit der Regierung und ihre Verantwortlichkeit gegenüber der Volksvertretung,

(noch Ziffer 19)

- e) die Unabhängigkeit der Gerichte,
- f) der Ausschluß jeder Gewalt- und Willkürherrschaft
und
- g) die im Grundgesetz konkretisierten Menschenrechte.

(3) Auswärtige Belange im Sinne des § 3 Abs. 1 Nr. 3 werden gefährdet, wenn innerhalb des Geltungsbereichs des Grundgesetzes Gewalt ausgeübt oder durch Handlungen vorbereitet wird und sich dies gegen die politische Ordnung oder Einrichtungen anderer Staaten richtet."

Begründung:

§ 3 Abs. 2 definiert nur die Bestrebungen gegen die freiheitlich demokratische Grundordnung und läßt dabei die politische Motivation unberücksichtigt.

Die vorgeschlagene Formulierung der Begriffsbestimmungen ist wesentlich umfassender. Sie dient der Präzisierung der Aufgabenbeschreibung und damit der gebotenen Normenklarheit. Sie greift die zentralen, von der Rechtsprechung immer wieder angesprochenen Elemente der freiheitlich-demokratischen Grundordnung auf.

20. Zu Artikel 2 (§ 3 BVerfSchG)

In Artikel 2 sind in § 3 Abs. 3 die Sätze 2 und 3 durch folgenden Satz zu ersetzen:

"Die Voraussetzungen und das Verfahren zur Durchführung einer Sicherheitsüberprüfung und Regelungen darüber, welche Umstände ein Sicherheitsrisiko begründen und welche Folgen für Bewerber und Beschäftigte beim Vorliegen eines Sicherheitsrisikos eintreten, werden in einem besonderen Gesetz geregelt."

Begründung:

Die Regelung des Absatzes 3 Sätze 2 und 3 ist unvollständig. Die Materie bedarf eingehender und normenklarer Regelung in einem besonderem Gesetz. In diesem Gesetz ist auch zu regeln, welche Personen in die Sicherheitsüberprüfung einbezogen werden. Der in der bisherigen Fassung des Satzes 3 verwendete Begriff "eheähnliche Gemeinschaft" ist im übrigen auch durch Auslegung nicht hinreichend bestimmbar..

21. Zu Artikel 2 (§§ 3b - neu - und 4)

a) In Artikel 2 ist nach § 3a - neu - folgender § 3b einzufügen:

"§ 3b

Abgrenzung der Zuständigkeiten der Verfassungsschutzbehörden

(1) Die Landesbehörden für Verfassungsschutz sammeln im Bereich ihres Landes Informationen, Auskünfte, Nachrichten und Unterlagen im Sinne des § 3 Abs. 1 und werten sie aus. Sie unterrichten das Bundesamt für Verfassungsschutz und die Landesbehörden für Verfassungsschutz über alle Ergebnisse ihrer Auswertung, die für sie von Bedeutung sind.

(noch Ziffer 21)

(2) Das Bundesamt für Verfassungsschutz kann in einem Lande im Benehmen mit der Landesbehörde für Verfassungsschutz Informationen, Auskünfte, Nachrichten und Unterlagen im Sinne des § 3 Abs. 1 **sammeln, wenn Bestrebungen** und Tätigkeiten im Sinne des § 3 Abs. 1 Nr. 1 bis 3

1. sich ganz oder überwiegend gegen den Bund richten,
2. sich über den Bereich eines Landes hinaus erstrecken,
3. auswärtige Belange des Bundes berühren
oder
4. wenn eine Landesbehörde für Verfassungsschutz das Bundesamt für Verfassungsschutz um ein Tätigwerden ersucht.

(3) Das Bundesamt für Verfassungsschutz unterrichtet die Landesbehörden für Verfassungsschutz über alle Unterlagen, deren Kenntnis für das Land zum Zwecke des Verfassungsschutzes erforderlich ist."

- b) In Artikel 2 ist
in § 4 der Absatz 1 zu streichen.

Begründung:

zu a:

Das Gesetz in der vorliegenden Fassung enthält keine Aufgabenabgrenzung zwischen dem Bundesamt für Verfassungsschutz und den Landesbehörden. Die aus der jetzigen Fassung abzuleitende Allzuständigkeit des Bundes verstößt gegen das föderative Prinzip und den in den Artikel 30 und 83 GG zum Ausdruck kommenden Rechtsgedanken, daß die Ausübung staatlicher Befugnisse und die Erfüllung der staatlichen Aufgaben Sache der Länder ist, soweit das Grundgesetz keine andere Regelung trifft oder vorsieht.

(noch Ziffer 21)

Nach Artikel 87 GG darf der Bund eine Zentralstelle zur Sammlung von Unterlagen des Verfassungsschutzes einrichten. Die allgemeine Zuständigkeit der Länder wird durch diese Befugnisnorm nicht berührt.

Eine Aufgabenabgrenzung muß aber auch aus dem Gesichtspunkt der Normenklarheit und der Festlegung der Verantwortlichkeiten als unverzichtbar angesehen werden. Die beantragte Regelung dieses wichtigen Problemkreises ist auf der Basis der bestehenden Koordinierungsrichtlinien formuliert worden. Diese Richtlinien können als verwaltungsinterne Absprachen allerdings nicht gesetzliche Zuständigkeitsfestlegungen ersetzen. Inhaltlich muß entsprechend den Intentionen des Grundgesetzes bestimmt werden, daß grundsätzlich die Zuständigkeit der Landesbehörden für Verfassungsschutz gegeben ist. Daneben bestehende Zuständigkeiten des Bundesamtes für Verfassungsschutz müssen möglichst präzise eingeschränkt werden.

zu b:

Folgeänderung.

22. Zu Artikel 2 (§ 4 BVerfSchG)

In Artikel 2 sind in § 4 Abs. 2 die Sätze 8 und 9 zu streichen.

Begründung:

Dateien mit Textzusätzen sind abzulehnen, da durch sie eine unkontrollierte Verbreitung von hochsensiblen Personal-
daten möglich ist.

23. Zu Artikel 2 (§ 6 BVerfSchG)

In Artikel 2 ist in § 6 Abs. 3 nach den Worten
"die Polizei"
die Worte
"und andere Behörden"
einzufügen.

Begründung:

Die Ergänzung dient der Klarstellung.

24. Zu Artikel 2 (§ 9 BVerfSchG)

In Artikel 2 sind in § 9 Abs. 2 die Worte
"In Dateien gespeicherte"
zu streichen.

Begründung:

Die Prüfung der Voraussetzungen einer Speicherung von
"Jugendsünden" muß sich auch auf Akten erstrecken.

25. Zu Artikel 2 (§ 10 BVerfSchG)

In Artikel 2 sind in § 10 Abs. 3 nach den Worten
"festgesetzten Fristen"

die Worte

", spätestens nach 5 Jahren"

einzufügen

und

folgender Satz anzufügen:

"Gespeicherte Daten über Bestrebungen nach § 3 Abs. 1
Nr. 1 oder 3 sind spätestens 10 Jahre nach dem Zeit-
punkt der letzten gespeicherten relevanten Information
zu löschen."

Begründung:

Die Formulierung "festgesetzte Fristen" ist nicht normen-
klar. Gesetzliche Fristen sind erforderlich. Die genannten
Fristen sind im Hinblick auf die Aufgabenerfüllung der Ver-
fassungsschutzbehörden angemessen.

26. Zu Artikel 2 (§ 13 BVerfSchG)

In Artikel 2 ist § 13 wie folgt zu ändern:

a) In Absatz 1 sind die Worte

" , soweit er hierzu auf einen konkreten Sachverhalt
hinweist und ein besonderes Interesse an einer
Auskunft darlegt "
zu streichen.

b) Die Absätze 2 bis 4 sind durch folgenden Absatz 2
zu ersetzen:

"(2) Absatz 1 gilt nicht, soweit eine Abwägung ergibt,
daß das Auskunftsrecht des Betroffenen gegenüber dem
öffentlichen Interesse an der Geheimhaltung der Tätig-
keit des Bundesamtes für Verfassungsschutz oder einem
überwiegenden Geheimhaltungsinteresse Dritter zurücktre-
ten muß. Die Entscheidung trifft der Behördenleiter oder
ein von ihm besonders beauftragter Mitarbeiter. Wird
die Auskunft nicht erteilt, ist der Betroffene
unter Mitteilung der wesentlichen Gründe darauf hinzu-
weisen, daß er sich an den Bundesbeauftragten für
den Datenschutz wenden kann. Die Verfassungsschutzbehörde
braucht die Auskunftsverweigerung nicht zu begründen, soweit
dadurch der Zweck der Auskunftsverweigerung gefährdet würde.
Die Gründe der Auskunftsverweigerung sind aktenkundig zu
machen."

Begründung:

Die vorgesehenen Regelungen tragen dem Informationsrecht des
Betroffenen nicht ausreichend Rechnung. Die Einführung einer
Begründungspflicht für ein Auskunftsbegehren schafft eine
Darlegungslast, die das Datenschutzrecht nicht kennt und die
neben dem Auskunftsverweigerungsrecht als übermäßige Sicherung
erscheint.

Die Inanspruchnahme des Auskunftsverweigerungsrechtes bedarf
der Entscheidung durch die Leitungsebene und erfordert zur
Sicherung der Nachprüfbarkeit eine Begründung.

27. Zu Artikel 2 (§ 16 BVerfSchG)

In Artikel 2 ist in § 16 der Absatz 4 wie folgt zu fassen:

"(4) Würden durch die Übermittlung nach Absatz 3 Satz 1 der Zweck der Maßnahme gefährdet oder Betroffene unverhältnismäßig beeinträchtigt, darf das Bundesamt für Verfassungsschutz bei der Wahrnehmung der Aufgaben nach § 3 Abs. 1 Nr. 2 und 3 sowie bei der Beobachtung terroristischer Bestrebungen amtliche Register einsehen."

Begründung:

Durch die Einsichtnahme in Register können die schutzwürdigen Belange Unbeteiligter beeinträchtigt werden. Der Grundsatz der Verhältnismäßigkeit gebietet deshalb eine Beschränkung der Befugnis.

28. Zu Artikel 2 (§ 17 BVerfSchG)

In Artikel 2 ist in § 17 der Absatz 2 wie folgt zu fassen:

"(2) Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an Dienststellen der Stationierungstreitkräfte übermitteln, soweit die Bundesrepublik Deutschland dazu im Rahmen von Artikel 3 des Zusatzabkommens zu dem Abkommen zwischen den Parteien des Nordatlantikpakt über die Rechtsstellung ihrer Truppen hinsichtlich der in der Bundesrepublik Deutschland stationierten ausländischen Streitkräfte vom 3. August 1959 (BGBl. 1961 II S. 1183) verpflichtet ist und sofern die Empfänger sich verpflichtet haben oder verpflichten, diese Daten nur zu diesen Zwecken zu verwenden."

Begründung:

Die Regelung in der Fassung des Gesetzesbeschlusses ist zum Schutz der sensiblen Daten nicht geeignet. Die Empfänger müssen die Zweckbindung aus Gründen des Datenschutzes akzeptieren..

29. Zu Artikel 2 (§ 17 BVerfSchG)

In Artikel 2 sind in § 17 Abs. 3
nach Satz 1 folgender Satz einzufügen:

"Die Übermittlung unterbleibt, sofern der Empfänger nicht
die erforderlichen Maßnahmen zur Verwirklichung der Grundsätze
des Übereinkommens des Europarates über den Schutz der Menschen
bei der automatischen Verarbeitung personenbezogener Daten
vom 29.01.1981 oder vergleichbare Regelungen getroffen hat."

sowie im bisherigen Satz 2 die Worte
"Die Übermittlung unterbleibt"
durch die Worte
"Sie unterbleibt auch"
zu ersetzen.

Begründung:

Die Ergänzung ist erforderlich zum Schutz der Betroffenen
vor Verletzungen des informationellen Selbstbestimmungsrechtes
durch rechtlich nicht hinreichend gebundene Empfänger.

30. Zu Artikel 2 (§ 17 BVerfSchG)

In Artikel 2 sind in § 17 Abs. 4 die Sätze 3 und 4 wie folgt zu fassen:

"Voraussetzung der Übermittlung ist, daß der Empfänger sich verpflichtet, die übermittelten Daten nur für den Zweck zu verwenden, zu dem sie ihm übermittelt worden sind, und sich bereit erklärt, dem Bundesamt für Verfassungsschutz Auskunft über die Verwendung der Daten auf Verlangen zu erteilen.

Begründung:

Die Regelung in § 17 Abs. 4 Sätze 3 und 4 in der Fassung des Gesetzesbeschlusses ist zum Schutze der sensiblen Daten nicht geeignet. Die Empfänger müssen die Zweckbindung aus Gründen des Datenschutzes akzeptieren.

31. Zu Artikel 2 (§ 24 BVerfSchG)

In Artikel 2 sind in § 24 die Worte
", wenn dies zur Wahrung schutzwürdiger Interessen
des Betroffenen erforderlich ist"
zu streichen.

Begründung:

Unrichtige Mitteilungen einer Behörde sind nach Kenntnis ihrer Unrichtigkeit unverzüglich zu korrigieren. Dies ist auch erforderlich, um sicherzustellen, daß der Empfänger nicht mit falschen Daten arbeitet und daß die falschen Daten nicht weiter übermittelt werden.

32. Zu Artikel 2 (§ 25 BVerfSchG)

In Artikel 2 ist § 25 zu streichen.

Begründung:

Die materiellen Voraussetzungen dieser Bestimmung

- es droht eine erhebliche Beeinträchtigung der freiheitlichen demokratischen Grundordnung
- oder
- es besteht eine konkrete Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes

sind nach ihrem Wortlaut sehr hoch. Wenn solche "Lagen" eintreten, werden sie mit den Mitteln des § 25 nicht zu beherrschen sein. Schon deshalb sollte die vorgesehene Regelung entfallen. Es besteht jedoch auch die Gefahr, daß die Vorschrift "großzügig" ausgelegt wird und auch in weniger schwerwiegenden Fällen zur Einrichtung von grundsätzlich unerwünschten on-line-Anschlüssen führt.

Es bestehen darüber hinaus erhebliche Zweifel, ob der vorgesehene on-line-Verbund ein zwecktaugliches Mittel ist. Um polizeiliche Dateien, insbesondere die PIOS-Dateien des INPOL-Systems und vergleichbare Anwendungen bei den Landeskriminalämtern wirksam nutzen zu können, ist eine gründliche Schulung erforderlich. Auch bedarf es eines längeren Erfahrungszeitraums, um die sich aus der Recherche im Einzelfall ergebenden Erkenntnisse zu bewerten. Aus diesen Gründen kann es nicht sinnvoll sein, daß Verfassungsschutzbehörden und Polizeibehörden jeweils Personal ausbilden, um für den Fall des § 25 mit den Dateien der jeweils anderen Behörden arbeiten zu können. Hierbei ist auch zu berücksichtigen, daß die technischen Gegebenheiten sich bei den einzelnen Dateien laufend ändern und daher eine fortlaufende Nachschulung des Personals notwendig wird.

33. Zu Artikel 3 (§ 1 MADG)

In Artikel 3 ist § 1 wie folgt zu ändern:

- a) Absatz 1 ist zu streichen.
- b) In Absatz 2 sind in Satz 1 nach den Worten
"Militärischen Abschirmdienstes"
die Worte
"des Bundesministers für Verteidigung"
einzufügen.

Begründung:

zu a:

Die Aufgabe des MAD ist in Absatz 2 hinreichend umschrieben. Absatz 1 könnte dahin mißverstanden werden, daß auch der MAD eine Verfassungsschutzbehörde mit umfassenden Aufgaben und Befugnissen wäre.

zu b:

Folge aus der Streichung des Absatzes 1.

34. Zu Artikel 3 (§ 1 MADG)

In Artikel 3 sind in § 1 Abs. 2
in Satz 1
die Nummer 1,
die Ordnungsnummer "2."
und
die Worte "Bestrebungen oder"

sowie

Satz 2 zu streichen.

Begründung:

Die hier genannte Aufgabe obliegt den Verfassungsschutzbehörden. Diese können sie auch im Geschäftsbereich des Bundesministers der Verteidigung - notfalls mit Amtshilfe des MAD - wahrnehmen. Für die in Nummer 2 umschriebene Aufgabe gilt dies nicht im gleichen Maße.

35. Zu Artikel 3 (§ 1 MADG)

In Artikel 3 sind in § 1 Abs. 4 die Sätze 2 und 3
durch folgenden Satz zu ersetzen:

"Die Voraussetzungen und das Verfahren zur Durchführung einer Sicherheitsüberprüfung und Regelungen darüber, welche Umstände ein Sicherheitsrisiko begründen und welche Folgen für Bewerber und Beschäftigte bei Vorliegen eines Sicherheitsrisikos eintreten, werden in einem besonderen Gesetz geregelt."

Begründung:

Siehe die Begründung zum Änderungsvorschlag zu § 3
Abs. 3 Sätze 2 und 3 BVerfSchG.

36. Zu Artikel 3 (§ 4 MADG)

In Artikel 3 sind in § 4 Abs. 2 nach den Worten
"die Polizei"
die Worte
"und andere Behörden"
einzufügen.

Begründung:

Klarstellung.

37. Zu Artikel 4 (§ 2 BNDG)

In Artikel 4 sind in § 2 Abs. 3 Satz 2 nach den Worten
"die Polizei"
die Worte
"und andere Behörden"
einzufügen.

Begründung:

Klarstellung.

38. Zu Artikel 5 - neu - (§ 69 SGB X)

a) Nach Artikel 4 ist folgender Artikel 5 einzufügen:

Artikel 5

Änderung des Zehnten Buches Sozialgesetzbuch

Das Zehnte Buch Sozialgesetzbuch (Artikel I des Gesetzes vom 18. August 1980, BGBl. I S. 1469, 2218), zuletzt geändert durch Artikel 10 des Gesetzes vom 20. Dezember 1988 (BGBl. I S. 2330), wird wie folgt geändert:

In § 69 Abs. 2 wird am Schluß der Punkt durch ein Komma ersetzt und folgende Nummer 3 angefügt:

"3. die Bezügestellen des öffentlichen Dienstes, soweit sie kindergeldabhängige Leistungen des Besoldungs-, Versorgungs- und Tarifrechts unter Verwendung von personenbezogenen Kindergelddaten festzusetzen haben, und deren aufsichts-, rechnungsprüfungs- oder weisungsberechtigte Behörden."

b) Die bisherigen Artikel 5 und 6 werden Artikel 6 und 7.

379/90

(noch Ziffer 38)

Begründung:

zu a:

Die Bezügestellen des öffentlichen Dienstes sind zwar seit 1975 für die Zahlung von Kindergeld an Bedienstete und Versorgungsempfänger des öffentlichen Dienstes zuständig. Sie waren aber zunächst in der Zuständigkeitsregelung des § 25 SGB I nicht förmlich als Träger für die Kindergeldzahlung festgelegt. Dies führte zunächst zu einer Sonderstellung in bestimmten Verfahrensfragen, z.B. hinsichtlich des Sozialdatenschutzes. Durch das 1. SGBÄndG vom 20. Juli 1988 (BGBl. I S. 1046) ist § 25 SGB I dahin geändert worden, daß nunmehr auch die Bezügestellen des öffentlichen Dienstes mit allen Konsequenzen als Leistungsträger festgelegt sind. Damit gelten für sie auch die Vorschriften über den Schutz der Sozialdaten, soweit sie Kindergeld zahlen, uneingeschränkt (u.a. §§ 67 ff SGB X). Diese lassen eine Offenbarung von Kindergelddaten für die Festsetzung dienstrechtlicher Bezüge an sich nicht zu, wie sie aber wegen der engen gesetzlichen und tarifrechtlichen Abhängigkeit dienstrechtlicher Ansprüche auf Ortszuschlag, Sozialzuschlag usw. vom Kindergeldanspruch unverzichtbar ist. Aus diesem Grunde müssen die im Rahmen des § 69 SGB X bereits bestehenden Offenbarungsbefugnisse durch eine spezielle Regelung ergänzt werden, die sich auf das zum Gesetzes- und Tarifvollzug unbedingt erforderliche Maß beschränkt.

Der Antrag zu a ist identisch mit dem vom Bundesrat im ersten Durchgang beschlossenen Änderungsvorschlag (BR-Drs. 618/88 (Beschluß), C Ziff. 85 - § 69 SGB X -), dem die Bundesregierung zugestimmt hat (BT-Drs. 11/4306 vom 06.04.1989, Anlage 3, Zu C. 85). Dieser Vorschlag ist nach Mitteilung des Bundesministers des Innern lediglich aufgrund eines Redaktionsversehens nicht in die Beratungen des Bundestages einbezogen worden.

zu b:

Folgeänderung.