Thüringen

(Freistaat Thüringen)

Thüringer Datenschutzgesetz (ThürDSG)

Neubekanntmachung vom 10. Oktober 2001 (GVBl. S. 276)

Inhaltsübersicht

Erster Abschnitt:
Allgemeine Bestimmungen

§ 1 Zweck des Gesetzes
§ 2 Anwendungsbereich
§ 3 Begriffsbestimmungen
§ 4 Zulässigkeit der Datenverarbeitung und -nutzung
§ 5 Rechte des Betroffenen
§ 5a Automatisierte Einzelentscheidung
§ 6 Datengeheimnis
§ 7 Automatisiertes Abrufverfahren
§ 8 Verarbeitung oder Nutzung personenbezogener Daten im Auftrag
§ 9 Technische und organisatorische Maßnahmen
§ 10 Anlagen- und Verfahrensverzeichnis
§ 10a Beauftragter für den Datenschutz

Zweiter Abschnitt
Schutzrechte

§ 11 Anrufung des Landesbeauftragten für den Datenschutz
§ 12 (aufgehoben)
§ 13 Auskunft an den Betroffenen
§ 14 Berichtigungsanspruch
§ 15 Anspruch auf Sperrung
§ 16 Anspruch auf Löschung
§ 17 Benachrichtigung bei regelmäßigen Datenübermittlungen
§ 18 Anspruch auf Schadensersatz

Dritter Abschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 19 Datenerhebung
§ 20 Datenspeicherung, -veränderung und -nutzung
§ 21 Datenübermittlung innerhalb des öffentlichen Bereichs
§ 22 Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs
§ 23 Datenübermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes
§ 24 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen
§ 25 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

Vierter Abschnitt
Besondere Bestimmungen

§ 26 Öffentliche Stellen, die am Wettbewerb teilnehmen
§ 27 Öffentlich-rechtliche Religionsgesellschaften
§ 28 Verarbeitung personenbezogener Daten durch den Rundfunk
§ 29 Beauftragter für den Datenschutz im Rundfunk
§ 30 Personenbezogene Daten aus ehemaligen Einrichtungen

§ 31 Verarbeitung personenbezogener Daten aus ehemaligen Einrichtungen
§ 32 Widerspruchsrecht
§ 33 (aufgehoben)

Fünfter Abschnitt
Überwachung des Datenschutzes bei öffentlichen Stellen

§ 34 Sicherstellung des Datenschutzes
§ 35 Bestellung des Landesbeauftragten für den Datenschutz
§ 36 Rechtsstellung und Verschwiegenheitspflicht
§ 36a Anwendung beamtenrechtlicher Vorschriften
§ 37 Kontrolle durch den Landesbeauftragten für den Datenschutz
§ 38 Pflicht zur Unterstützung
§ 39 Beanstandung durch den Landesbeauftragten für den Datenschutz
§ 40 Weitere Aufgaben des Landesbeauftragten für den Datenschutz
§ 41 Beirat beim Landesbeauftragten für den Datenschutz

Sechster Abschnitt
Aufsichtsbehörden für die Datenverarbeitung nichtöffentlicher Stellen

§ 42 Aufsichtsbehörde

Siebter Abschnitt
Strafbestimmung, Übergangs- und Schlussbestimmungen

§ 43 Strafbestimmung
§ 43a Übergangsbestimmungen
§ 43b Gleichstellungsbestimmung
§ 44 In-Kraft-Treten

Erster Abschnitt
Allgemeine Bestimmungen

§ 1
Zweck des Gesetzes

Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten durch öffentliche Stellen (§ 2 Abs. 1 und) in seinem Persönlichkeitsrecht beeinträchtigt wird.

§ 2
Anwendungsbereich

(1) Die Bestimmungen dieses Gesetzes gelten für die Verarbeitung und Nutzung personenbezogener Daten durch die Behörden, die Gerichte und die sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen).

(2) Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts beteiligt sind. Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts, auf die dieses Gesetz nach Satz 1 Anwendung findet, an einer weiteren Vereinigung des privaten Rechts, so findet Satz 1 entsprechende Anwendung. Nehmen nicht öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes.

(3) Soweit besondere Rechtsvorschriften des Bundes oder des Landes auf personenbezogene Daten anzuwenden sind, gehen sie den Bestimmungen dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten und von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Bestimmungen dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet oder genutzt werden.

(5) Die Bestimmungen dieses Gesetzes gelten für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird. Verwaltungsangelegenheiten des Landtags sind insbesondere

1. die wirtschaftlichen Angelegenheiten des Landtags nach Artikel 57 Abs. 4 Satz 1 der Verfassung des Freistaats Thüringen,

2. die Personalverwaltung des Landtags,

3. die Ausübung des Hausrechts und der Ordnungs- und Polizeigewalt nach Artikel 57 Abs. 3 Satz 2 der Verfassung des Freistaats Thüringen und

4. die Ausführung der Gesetze, soweit diese dem Präsidenten des Landtags zugewiesen ist und nicht in unmittelbarem Zusammenhang mit der Wahrnehmung parlamentarischer Aufgaben steht.

Für die Verarbeitung und Nutzung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Landtag einschließlich der Fraktionen finden die Bestimmungen dieses Gesetzes unter Berücksichtigung der verfassungsrechtlichen Stellung des Landtags entsprechende Anwendung. Soweit der Landtag in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeitet oder nutzt, wird die Einhaltung des Datenschutzes durch den Ältestenrat des Landtags kontrolliert.

(6) Für die Gerichte und den Rechnungshof gelten die §§ 10 und 11 sowie der Fünfte Abschnitt nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

§ 3
Begriffsbestimmungen

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

(2) Automatisiert im Sinne dieses Gesetzes ist das Verarbeiten oder Nutzen personenbezogener Daten, wenn es unter Einsatz eines gesteuerten technischen Verfahrens durchgeführt wird.

(3) Verarbeiten ist das Erheben, Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren,

1. Erheben das Beschaffen von Daten über den Betroffenen,

2. Speichern das Erfassen, Aufnehmen oder Aufbewahren personen-bezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,

3. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

4. Übermitteln die Bekanntgabe gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an Dritte in der Weise, dass

    a) die Daten durch die Daten verarbeitende Stelle an den

Dritten weitergegeben werden oder

b) der Dritte von der Daten verarbeitenden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

5. Sperren das Kennzeichnen gespeicherter personenbezogener Daten um ihre weitere Verarbeitung oder Nutzung einzuschränken,

6. Löschen das endgültige Unkenntlichmachen gespeicherter personenbezogener Daten.

(4) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um die Verarbeitung handelt, insbesondere die Weitergabe von Daten innerhalb der Daten verarbeitenden Stelle an Teile derselben Stelle mit anderen Aufgaben oder anderem örtlichen Zuständigkeitsbereich.

(5) Daten verarbeitende Stelle ist jede öffentliche Stelle, die Daten in eigener Verantwortung für sich selbst verarbeitet oder nutzt oder dies im Auftrag durch andere vornehmen lässt.

(6) Empfänger ist jede Person oder Stelle, die Daten über den Betroffenen erhält. Dritter ist jede Person oder Stelle außerhalb der Daten verarbeitenden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen oder Stellen, die im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedsstaaten der Europäischen Union personenbezogene Daten im Auftrag verarbeiten oder nutzen.

(7) Eine Datei ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich ist, unabhängig davon, ob sie durch automatisierte Verfahren ausgewertet werden kann

(automatisierte Datei) oder nicht (nicht automatisierte Datei).

(8) Eine Akte ist jede sonstige der Aufgabenerfüllung dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(9) 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 bestimmbaren natürlichen Person zugeordnet werden können.

(10) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen ohne Nutzung der Zuordnungsfunktion auszuschließen oder wesentlich zu erschweren.

§ 4
Zulässigkeit der Datenverarbeitung und -nutzung

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

(2) Einwilligung ist die auf freiwilliger Entscheidung beruhende Willenserklärung des Betroffenen, einer bestimmten, seine personenbezogenen Daten betreffenden Verarbeitung oder Nutzung zuzustimmen.

(3) Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Verarbeitung oder Nutzung 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.

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

(5) Das Verarbeiten oder Nutzen von personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Daten über Gesundheit oder Sexualleben (besonders geschützte Daten) ist nur zulässig, wenn

1. eine Rechtsvorschrift dies ausdrücklich vorsieht oder zwingend voraussetzt,

2. die Betroffenen eingewilligt haben, wobei sich die Einwilligung ausdrücklich auf diese Daten beziehen muss,

3. es zum Schutz lebenswichtiger Interessen Betroffener oder Dritter erforderlich ist, sofern die Betroffenen aus physischen oder rechtlichen Gründen außerstande sind, ihre Einwilligung zu geben,

4. es sich um Daten handelt, die Betroffene offenkundig öffentlich gemacht haben,

5. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und Ordnung erforderlich ist,

6. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an dem Abschluss des Forschungsvorhabens das Interesse des Betroffenen an dem Aus-

schluss der Verarbeitung oder Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,

7. es erforderlich ist, um den Rechten und Pflichten der öffentlichen Stellen auf dem Gebiet des Dienst- und Arbeitsrechts Rechnung zu tragen, oder

8. es zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. § 27 bleibt unberührt.

(6) Begründet der Betroffene schriftlich, dass der rechtmäßigen Verarbeitung oder Nutzung seiner Daten schutzwürdige, sich aus seiner besonderen persönlichen Lage ergebende Interessen entgegenstehen, ist die Verarbeitung oder Nutzung aufgrund dieses Gesetzes nur zulässig, nachdem eine Abwägung im Einzelfall ergeben hat, dass seine Gründe hinter dem Interesse an der Verarbeitung oder Nutzung zurückstehen müssen. Dem Betroffenen ist das Ergebnis mit Begründung schriftlich mitzuteilen. Satz 1 gilt nicht, wenn eine Rechtsvorschrift die Verarbeitung oder Nutzung zwingend anordnet.

(7) Die Absätze 5 und 6 gelten nicht für

1. das Landesamt für Verfassungsschutz im Rahmen seiner Aufgabenstellung nach § 2 des Thüringer Verfassungsschutzgesetzes (ThürVSG) vom 29. Oktober 1991 (GVBl. S. 527) in der jeweils geltenden Fassung,

2. Behörden der Gefahrenabwehr, der Strafverfolgung, des Justizvollzugs und der Gerichts- und Bewährungshilfe sowie

3. Gerichte, sofern die Verarbeitung personenbezogener Daten in nicht automatisierten Dateien erfolgt.

§ 5
Rechte des Betroffenen

(1) Der Betroffene hat nach Maßgabe dieses Gesetzes ein Recht auf:

1. Anrufung des Landesbeauftragten für den Datenschutz (§ 11),
2. Einsicht in das Verfahrensverzeichnis (§ 10),
3. Auskunft über die zu seiner Person gespeicherten Daten (§ 13),
4. Berichtigung, Sperrung und Löschung der zu seiner Person gespeicherten Daten (§§ 14 bis 16),
5. Benachrichtigung bei regelmäßigen Datenübermittlungen (§ 17),
6. Schadensersatz (§ 18),
7. Einwände gegen die Verarbeitung seiner personenbezogenen Daten (§ 4 Abs. 6),
8. Auskunft bei automatisierten Einzelentscheidungen (§ 5 a).

(2) Diese Rechte können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(3) Sind an der Verarbeitung der Daten des Betroffenen mehrere Stellen beteiligt, so kann er sich an jede dieser Stellen wenden. Jede Stelle ist verpflichtet, das Vorbringen des Betroffenen an die zuständige Stelle weiterzuleiten. Der Betroffene ist über die Weiterleitung und die zuständige Stelle zu unterrichten. Die Sätze 2 und 3 gelten nicht, soweit

eine Auskunftserteilung aufgrund des § 13 Abs. 5 unterbleibt oder es sich um ein Auskunftsersuchen nach § 11 ThürVSG handelt.

(4) Wird für den Erhalt einer Leistung, das Erkennen einer Person oder für einen anderen Zweck ein Datenträger herausgegeben, den der Inhaber mit sich führen kann und auf dem seine personenbezogenen Daten automatisiert verarbeitet werden, hat die Daten verarbeitende Stelle sicherzustellen, dass er dies erkennen und seine ihm nach Absatz 1 zustehenden Rechte ohne unvertretbaren Aufwand geltend machen kann. Der Inhaber ist bei Herausgabe des Datenträgers über die ihm nach Absatz 1 zustehenden Rechte sowie über die von ihm bei Verlust des Datenträgers zu treffenden Maßnahmen und über die Folgen aufzuklären.

§ 5 a
Automatisierte Einzelentscheidung

Soweit gesetzlich nichts anderes bestimmt ist oder anderslautende Vereinbarungen zwischen der Daten verarbeitenden Stelle und dem Betroffenen nicht erfolgt sind, dürfen Entscheidungen, die für den Betroffenen rechtliche Folgen haben und ihn erheblich beeinträchtigen, nicht ausschließlich aufgrund automatisierter Verarbeitung oder Nutzung der Daten zum Zwecke der Bewertung einzelner Aspekte seiner Person ergehen.

§ 6
Datengeheimnis

Den bei Daten verarbeitenden Stellen beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu

nutzen (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 7
Automatisiertes Abrufverfahren

(1) Ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, darf nur eingerichtet werden, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Soll ein solches Verfahren die Übermittlung personenbezogener Daten ermöglichen, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, so darf es nur eingerichtet werden, soweit dies eine Rechtsvorschrift zulässt.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,

2. Dritte, denen die Übermittlung personenbezogener Daten durch Abruf ermöglicht wird,

3. Art der abzurufenden Daten,

4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

Die erforderlichen Festlegungen können auch durch die Fachaufsichtsbehörde mit Wirkung für ihrer Aufsicht unterliegende Stellen des Landes getroffen werden.

(3) Über die Einrichtung eines Abrufverfahrens ist vorher der Landesbeauftragte für den Datenschutz unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung eines Abrufverfahrens, an dem die in § 13 Abs. 4 genannten Stellen beteiligt sind, bedarf der Zustimmung des für die Daten verarbeitende und die abrufende Stelle jeweils zuständigen Ministeriums.

(4) Die Zulässigkeit des einzelnen Abrufs beurteilt sich nach den für die Erhebung und Übermittlung geltenden Vorschriften. Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt die abrufende Stelle. Die Daten verarbeitende Stelle prüft die Zulässigkeit des Abrufs nur, wenn dazu Anlass besteht. Die Daten verarbeitende 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 ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

(6) Die Absätze 1, 2 und 4 gelten entsprechend, wenn innerhalb einer Daten verarbeitenden Stelle ein automatisiertes Abrufverfahren eingerichtet wird.

§ 8
Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag öffentlicher Stellen durch andere Personen oder Stellen verarbeitet oder genutzt, bleibt der Auftraggeber für die Einhaltung der Bestimmungen dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 13 bis 18 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftraggeber hat den Auftragnehmer unter besonderer Berücksichtigung der Eignung der von diesem 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. Der Auftraggeber hat sich von der Einhaltung der Maßnahmen nach Satz 2 zu überzeugen. Vom Auftraggeber veranlasste Kontrollen hat der Auftragnehmer jederzeit zu ermöglichen. Der Auftrag kann auch durch die Fachaufsichtsbehörde mit Wirkung für ihrer Aufsicht unterliegenden Stellen des Landes erteilt werden; diese sind von der Auftragserteilung zu unterrichten.

(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) Ist der Auftragnehmer eine öffentliche Stelle, gelten für ihn nur die §§ 6, 9, 10, 10a, 34, 37 bis 40 und 43.

(5) Soweit juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen dem Land oder einer

der Aufsicht des Landes unterstehenden Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, für eine öffentliche Stelle Daten im Auftrag verarbeiten, gelten die §§ 10, 34 und 37 bis 40 entsprechend.

(6) Sind auf den Auftragnehmer die Bestimmungen dieses Gesetzes nicht anwendbar, hat der Auftraggeber die für die Einhaltung des Datenschutzes beim Auftragnehmer zuständige Kontrollstelle über die Beauftragung zu unterrichten.

(7) Die Absätze 1 bis 5 gelten entsprechend für die Wartung oder Fernwartung automatisierter Datenverarbeitungsanlagen, soweit ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

§ 9
Technische und organisatorische Maßnahmen

(1) Öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Bestimmungen dieses Gesetzes zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(2) Die zu treffenden technischen und organisatorischen Maßnahmen sind auf der Grundlage eines Sicherheitskonzepts zu ermitteln und haben je nach der Art der zu schützenden Daten zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),

2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),

3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),

4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),

5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit),

6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

Die Wirksamkeit der Maßnahmen ist unter Berücksichtigung sich verändernder Rahmenbedingungen und der Entwicklung der Technik zu überprüfen. Die sich daraus ergebenden notwendigen Anpassungen sind zeitnah umzusetzen.

§ 10
Anlagen- und Verfahrensverzeichnis

(1) Die Daten verarbeitenden Stellen führen ein Verzeichnis der automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden. Das Verzeichnis kann auch bei einer Daten verarbeitenden Stelle für andere Stellen geführt werden.

(2) In dem Verzeichnis ist für jedes automatisierte Verfahren schriftlich festzulegen:

1. Name und Anschrift der Daten verarbeitenden Stelle,

2. die Bezeichnung des Verfahrens,

3. die Aufgabe, zu deren Erfüllung personenbezogene Daten verarbeitet werden und die Rechtsgrundlage der Verarbeitung,

4. die Art der gespeicherten Daten,

5. der Kreis der Betroffenen,

6. die Art der regelmäßig zu übermittelnden Daten und deren Empfänger sowie geplante Übermittlungen in Drittstaaten,

7. die Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung,

8. die verarbeitungsberechtigten Personen oder Personengruppen,

9. eine allgemeine Beschreibung des Datenverarbeitungssystems, die eine vorläufige Beurteilung der Angemessenheit der nach § 9 getroffenen Maßnahmen erlaubt.

(3) Das Verzeichnis kann mit Ausnahme der Angaben zu den Nummern 8 und 9 von jedermann gebühren- und auslagenfrei eingesehen werden. Dies gilt nicht für Verfahrensverzeichnisse der Verfassungsschutzbehörden sowie bei Vorliegen von Versagungsgründen nach § 13 Abs. 5.

(4) Verfahren nach § 34 Abs. 3 Satz 1 Nr. 3 und Satz 2, die einer Freigabe nicht bedürfen, finden keine Aufnahme in das Verfahrensverzeichnis.

§ 10 a
Beauftragter für den Datenschutz

(1) Daten verarbeitende Stellen, die personenbezogene Daten mit Hilfe automatisierter Verfahren verarbeiten oder nutzen, haben einen ihrer Beschäftigten zum Beauftragten für den Datenschutz schriftlich zu bestellen. Einer Bestellung eines Beauftragten für den Datenschutz bedarf es nicht, wenn in der Daten verarbeitenden Stelle ausschließlich Verfahren der in § 34 Abs. 3 genannten Art eingesetzt werden. Notare und die in § 2 Abs. 2 Satz 3 genannten Stellen haben einen Beauftragten erst dann einzusetzen, wenn mindestens fünf Personen bei der automatisierten Verarbeitung oder Nutzung personenbezogener Daten beschäftigt werden. Bestellt werden darf nur, wer die notwendige Fachkenntnis in Fragen des Datenschutzes und der Datensicherheit hat und durch diese Tätigkeit keinem unüberwindbaren Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird.

(2) Der Beauftragte für den Datenschutz ist in dieser Funktion dem Leiter der Daten verarbeitenden Stelle unmittelbar zu unterstellen und hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung dieses Gesetzes und anderer Rechtsvorschriften über den Datenschutz zu unterstützen und auf deren Einhaltung hinzuwirken. In seiner Eigenschaft als Beauftragter für den Datenschutz ist er nicht weisungsgebunden. Zu seinen Aufgaben gehört insbesondere

1. bei der Freigabe automatisierter Verfahren nach § 34 Abs. 2 mitzuwirken,

2. das Verfahrensverzeichnis nach § 10 zu führen,

3. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden, zu überwachen und

4. die Beratung der bei der Verarbeitung oder Nutzung personenbezogener Daten tätigen Personen zu den Bestimmungen dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sowie den sich hieraus ergebenden besonderen Erfordernissen.

(3) Die Daten verarbeitende Stelle hat den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben in geeigneter Weise zu unterstützen und ihm insbesondere die zur Erfüllung seiner Aufgaben erforderlichen Sachmittel und Räumlichkeiten zur Verfügung zu stellen.

(4) Der Beauftragte für den Datenschutz darf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung und dem Arztgeheimnis, sowie personenbezogene Daten in Personalakten und in Akten über die Sicherheitsüberprüfung nur mit Einwilligung der Betroffenen einsehen. Die Einsicht in Unterlagen, die solche Daten enthalten, die die Sicherheit des Bundes oder eines Landes gefährden könnten, ist nur im Benehmen mit dem Leiter der Daten verarbeitenden Stelle zulässig.

(5) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über die Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er hiervon nicht durch den Betroffenen befreit wird. Dies gilt auch nach Beendigung der Tätigkeit als Beauftragter für den Datenschutz.

(6) Für mehrere Daten verarbeitende Stellen kann ein gemeinsamer Beauftragter für den Datenschutz bestellt werden.

(7) § 29 bleibt unberührt.

Zweiter Abschnitt
Schutzrechte

§ 11
Anrufung des Landesbeauftragten für den Datenschutz

(1) Jedermann kann sich, unbeschadet des allgemeinen Petitionsrechts oder anderer Rechte, unmittelbar an den Landesbeauftragten für den Datenschutz mit dem Vorbringen wenden, dass bei der Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen seine schutzwürdigen Belange beeinträchtigt werden.

(2) Niemand darf benachteiligt oder gemaßregelt werden, weil er von seinem Recht nach Absatz 1 Gebrauch gemacht hat.

(3) Wendet sich ein Betroffener an den Landesbeauftragten für den Datenschutz, weil ihm nach § 13 Abs. 5 oder besonderen gesetzlichen Vorschriften keine Auskunft erteilt worden ist, darf die Mitteilung des Landesbeauftragten an den Betroffenen keine Rückschlüsse auf den Erkenntnisstand der Daten verarbeitenden Stelle zulassen, sofern diese nicht einer weiter gehenden Auskunft zustimmt. Das Gleiche gilt, wenn ein Betroffener unmittelbar den Landesbeauftragten anruft und die für die Erteilung der Auskunft zuständige Stelle diesem unter Angabe von Gründen darlegt, dass sie bei einem Auskunftsersuchen eine Auskunft nach den in Satz 1 genannten Vorschriften verweigern würde.

§ 12
(aufgehoben)

§ 13
Auskunft an den Betroffenen

(1) Die Daten verarbeitende Stelle hat dem Betroffenen auf Antrag ohne unzumutbare Verzögerung Auskunft zu erteilen über

1. die zu seiner Person verarbeiteten Daten,

2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie

3. die Herkunft der Daten und deren Empfänger oder die Kategorien der Empfänger, soweit diese Angaben gespeichert sind.

Dies gilt nicht für personenbezogene Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

(2) Für die Auskunft werden Verwaltungskosten nicht erhoben, es sei denn, dass mit der Auskunftserteilung ein besonderer Verwaltungsaufwand verbunden ist.

(3) In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten nur 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 Daten verarbeitende Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen; dabei dürfen berechtigte Interessen Dritter nicht beeinträchtigt werden.

(4) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Behörden der Staatsanwaltschaften, Polizeibehörden, an Verfassungsschutzbehörden, den Bundesnachrichten-

dienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung, so ist sie nur mit Zustimmung dieser Stellen zulässig.

(5) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgaben gefährden würde,

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

3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen den überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen,

4. die personenbezogenen Daten zur Entscheidung in Gnadensachen oder zur Entscheidung über die Verleihung von staatlichen Orden oder Ehrenzeichen gespeichert sind

und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(6) 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 Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Landesbeauftragten für den Datenschutz wenden kann.

(7) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht das zuständige Landesministerium im Einzelfall feststellt,

dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde.

§ 14
Berichtigungsanspruch

Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird bei personenbezogenen Daten in Akten festgestellt, daß sie unrichtig sind, oder wird ihre Richtigkeit vom Betroffenen bestritten, so ist dies in der Akte zu vermerken oder auf sonstige Weise festzuhalten.

§ 15
Anspruch auf Sperrung

Anspruch auf Sperrung

(1) Personenbezogene Daten in Dateien sind zu sperren, wenn

1. ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt oder

2. eine Löschung aus den in § 16 Abs. 4 genannten Gründen unterblieben ist.

(2) Personenbezogene Daten in Akten sind zu sperren, wenn die Daten verarbeitende Stelle im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörden nicht mehr erforderlich sind oder eine Löschung aus den in § 16 Abs. 4 genannten Gründen unterblieben ist.

(3) Ohne Einwilligung des Betroffenen dürfen gesperrte personenbezogene Daten nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot, zu Aufsichts- und Kontrollzwecken, zur Rechnungsprüfung oder aus sonstigen im überwiegenden Interesse der Daten verarbeitenden Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

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

Gesperrte personenbezogene Daten, deren Löschung nur nach § 16 Abs. 4 unterblieben ist, dürfen ohne Einwilligung des Betroffenen nicht mehr übermittelt oder genutzt werden.

§ 16
Anspruch auf Löschung

(1) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder

2. ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist.

(2) Sind personenbezogene Daten in Akten gespeichert, ist die Löschung nach Absatz 1 Nr. 2 nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist. Die Daten sind in diesem Fall bis zu ihrer Löschung entsprechend § 15 zu sperren.

(3) Vor einer Löschung sind die Daten nach Absatz 1 Nr. 2 dem zuständigen Archiv zur Übernahme anzubieten. Das Nähere wird durch Rechtsvorschriften über öffentliche Archive geregelt.

(4) Die Löschung unterbleibt, wenn

1. Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden,

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

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

(5) Nach § 15 Abs. 1 Nr. 2 gesperrte Daten sind nach Wegfall der in Absatz 4 genannten Gründe endgültig zu löschen.

§ 17
Benachrichtigung bei regelmäßigen Datenübermittlungen

Von einer Berichtigung unrichtiger Daten (§ 14), der Sperrung bestrittener Daten (§ 15 Abs. 1 Nr. 1) sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung (§ 16 Abs. 1 Nr. 1; § 15 Abs. 1 Nr. 2 in Verbindung mit § 16 Abs. 4 und Abs. 1 Nr. 1) sind die Stellen zu verständigen, denen im Rahmen einer regelmäßigen Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

§ 18
Anspruch auf Schadensersatz

(1) Fügt eine Daten verarbeitende Stelle einem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten einen Schaden zu, ist sie dem Betroffenen gegenüber zum Ersatz dieses Schadens verpflichtet. Die Ersatzpflicht entfällt, soweit die nach den Umständen des Falls gebotene Sorgfalt beachtet wurde.

(2) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(3) Auf das Mitverschulden des Betroffenen und die Verjährung sind die §§ 254 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

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

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

Dritter Abschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 19
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. die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder

3. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde.

In den Fällen der Nummern 2 und 3 ist eine Erhebung bei Dritten nur zulässig, wenn keine Anhaltspunkte dafür vorliegen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist die Identität der Daten verarbeitenden Stelle, der Erhebungszweck sowie im Fall vorgesehener Übermittlung der Empfänger der Daten 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. Wurden Daten ohne Kenntnis des Betroffenen erhoben, ist dieser in den Fällen des Absatzes 2 Satz 2 Nr. 2 und 3 bei der ersten Speicherung der Daten oder im Fall einer beabsichtigten Weitergabe der Daten an Dritte spätestens bei der ersten Übermittlung der Daten zu benachrichtigen. Dies gilt nicht, wenn eine Auskunft nach § 13 Abs. 5 unterbleiben würde oder eine Information des Betroffenen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert.

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

§ 20
Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der Daten verarbeitenden Stelle liegenden Aufgabe 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 der anderen Zwecke seine Einwilligung verweigern würde;

4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen;

5. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die Daten verarbeitenden Stelle sie veröffentlichen dürfte, es sei denn, daß das schutzwürdige Interesse des Betroffenen an dem Ausschluß der Zweckänderung überwiegt;

6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist;

7. 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 Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist;

8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

9. es zur Durchführung wissenschaftlicher Forschung 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.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Durchführung von Organisationsuntersuchungen, der Prüfung und Wartung von automatisierten Verfahren der

Datenverarbeitung oder der Erstellung von Geschäftsstatistiken für die speichernde Stelle dient. Dies gilt auch für die Verarbeitung und Nutzung zu Ausbildungs- und Prüfungszwecken durch die speichernde Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(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.

§ 21
Datenübermittlung innerhalb des öffentlichen Bereichs

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

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten liegenden Aufgaben erforderlich ist und

2. die Voraussetzungen vorliegen, die eine Nutzung nach § 20 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Falle prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

(3) Der Dritte, an den die Daten übermittelt werden, darf die übermittelten Daten 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 des § 20 Abs. 2 zulässig.

(4) 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 unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung überwiegen; eine Nutzung dieser Daten ist unzulässig.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn personenbezogene Daten innerhalb der Daten verarbeitenden Stelle weitergegeben werden oder wenn personenbezogene Daten von einer anderen öffentlichen Stelle im automatisierten Verfahren abgerufen werden.

§ 22
Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs

(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 § 20 zulassen würden, oder

2. der Dritte, an den die Daten übermittelt werden, 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, wenn die Unterrichtung wegen der Art der personenbezogenen Daten unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen nicht geboten erscheint oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt worden sind. Die übermittelnde Stelle hat ihn 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.

§ 23
Datenübermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes

(1) Für die Übermittlung personenbezogener Daten an öffentliche und nicht öffentliche Stellen im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedsstaaten der Europäischen Union sowie an Organe und Einrichtungen der Europäischen Gemeinschaften gelten die §§ 21 und 22 entsprechend. Für die Übermittlung personenbezogener Daten außerhalb des in Satz 1 genannten Bereichs (Drittstaaten) sowie an über- oder zwischenstaatliche Stellen gilt § 22 Abs. 1 und 3. Die Übermittlung ist darüber hinaus nur zulässig, wenn ein angemessenes Datenschutzniveau gewährleistet ist.

(2) Wenn in einem Drittstaat kein angemessenes Datenschutzniveau im Sinne des Absatzes 1 gewährleistet ist, so ist die Übermittlung personenbezogener Daten nur zulässig, soweit sie

1. zweifelsfrei mit Einwilligung des Betroffenen erfolgt,

2. für die Erfüllung eines Vertrags zwischen dem Betroffenen und der Daten verarbeitenden Stelle oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag des Betroffenen erforderlich ist,

3. zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der Daten verarbeitenden Stelle mit einem Dritten abgeschlossen wurde oder geschlossen werden soll,

4. entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist,

5. für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder

6. aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind.

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

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

(5) 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.

§ 24
Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unter

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Person oder Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der Daten verarbeitende Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat.

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

§ 25
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 öffentli-

che 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 Bestimmung 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 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, soweit

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

Vierter Abschnitt
Besondere Bestimmungen

§ 26
Öffentliche Stellen, die am Wettbewerb teilnehmen

Soweit öffentliche Stellen am Wettbewerb teilnehmen, sind auf sie, auf ihre Zusammenschlüsse und Verbände von den Bestimmungen dieses Gesetzes nur der Fünfte Abschnitt, ausgenommen § 34 Abs. 2, anzuwenden. Im Übrigen gelten für sie die Bestimmungen des Bundesdatenschutzgesetzes mit Ausnahme des Zweiten Abschnitts und des § 38.

§ 27
Öffentlich-rechtliche Religionsgesellschaften

Personenbezogene Daten dürfen in entsprechender Anwendung des § 21 von der Daten verarbitende Stelle an Stellen der öffentlich-rechtlichen Religionsgesellschaften übermittelt werden, wenn sichergestellt ist, daß beim Empfänger ausreichende Datenschutzmaßnahmen getroffen sind.

§ 28
Verarbeitung personenbezogener Daten durch den Rundfunk

(1) Soweit eine öffentlich-rechtliche Rundfunkanstalt des Landes personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet oder nutzt, gelten von den Bestimmungen dieses Gesetzes nur die §§ 6 und 9. Für die Verarbeitung personenbezogener Daten zu anderen Zwecken gelten neben

§ 29 die Bestimmungen dieses Gesetzes entsprechend mit Ausnahme des Fünften Abschnitts.

(2) Führt die journalistisch-redaktionelle Verarbeitung oder Nutzung personenbezogener Daten durch die Rundfunkanstalt zur Verbreitung einer Gegendarstellung des Betroffenen, so ist diese zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Rundfunkanstalt in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrunde liegenden, 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.

§ 29
Beauftragter für den Datenschutz im Rundfunk

(1) Der Intendant der Rundfunkanstalt beruft mit Zustimmung des Verwaltungsrates einen Beauftragten für den Datenschutz im Rundfunk.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Erfüllung seiner Aufgaben nach diesem Gesetz an Weisungen nicht gebunden; im übrigen untersteht er der Dienstaufsicht des Intendanten.

(3) Jedermann kann sich entsprechend § 11 Abs. 1 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) Bei Beanstandungen verständigt der Beauftragte für den Datenschutz den Intendanten und den Verwaltungsrat. Er erstattet den Organen des Rundfunks alle zwei Jahre einen Bericht über seine Tätigkeit; diesen übermittelt er auch dem Landesbeauftragten für den Datenschutz.

(5) Der Beauftragte für den Datenschutz hat, auch nach seinem Ausscheiden, über die ihm bei seiner Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

§ 30
Personenbezogene Daten aus ehemaligen Einrichtungen

(1) Personenbezogene Daten aus ehemaligen Einrichtungen, die vor dem 3. Oktober 1990 nach ihrer Zweckbestimmung überwiegend für Verwaltungsaufgaben gespeichert waren, die nach dem Grundgesetz von Ländern, Gemeinden, Gemeindeverbänden oder sonstigen Trägern öffentlicher Verwaltung wahrzunehmen sind, stehen demjenigen Träger öffentlicher Verwaltung zu, der nach dem Grundgesetz für die Verwaltungsaufgabe zuständig ist. Dieser bestimmt die verantwortliche Daten verarbeitende Stelle. In Zweifelsfällen wird die Daten verarbeitende Stelle durch die Landesregierung bestimmt.

(2) Ehemalige Einrichtungen im Sinne des Absatzes 1 sind ehemalige staatliche oder wirtschaftsleitende Organe, Kombinate, Betriebe oder Einrichtungen sowie gesellschaftliche Organisationen der Deutschen Demokratischen Republik.

§ 31
Verarbeitung personenbezogener Daten aus ehemaligen Einrichtungen

(1) Abweichend von § 20 Abs. 1 ist das Speichern, Verändern oder Nutzen personenbezogener Daten aus ehemaligen Einrichtungen durch die in § 30 Abs. 1 genannten Daten verarbeitenden Stellen zulässig, soweit

1. die Kenntnis der Daten zur rechtmäßigen Erfüllung einer in der Zuständigkeit dieser Stellen liegenden Aufgabe erforderlich ist,

2. die erneute Erhebung dieser Daten einen unverhältnismäßig hohen Aufwand darstellt,

3. der Betroffene der Verarbeitung oder Nutzung nicht nach § 32 widersprochen hat und

4. die Zuständigkeit und Verantwortlichkeit der Daten verarbeitenden Stellen eindeutig bestimmt ist.

Satz 1 gilt nicht für eine Verwendung der Daten zum Nachteil des Betroffenen, wenn anzunehmen ist, dass sie unter Verstoß gegen die Menschenwürde erhoben worden sind.

(2) Personenbezogene Daten, deren Verarbeitung und Nutzung nach Absatz 1 zulässig ist, gelten als für den nach Absatz 1 Nr. 1 bestimmten Zweck erstmalig eingespeichert.

§ 32
Widerspruchsrecht

(1) Der Betroffene kann der Verarbeitung und Nutzung seiner personenbezogenen Daten widersprechen, wenn die Daten ohne seine Mitwirkung durch eine ehemalige Einrichtung erhoben oder gespeichert wurden und die Daten nach geltendem Recht nicht ohne seine Mitwirkung erhoben werden dürfen oder wenn anzunehmen ist, daß sie unter Verstoß gegen die Menschenwürde erhoben worden sind.

(2) Der Betroffene ist in geeigneter Weise über

1. die Herkunft solcher Daten,
2. die Art der ursprünglichen Verwendung,
3. die Art und den Umfang der beabsichtigten Verarbeitung oder Nutzung,
4. die nunmehr zuständige Daten verarbeitende Stelle und
5. die bestehende Widerspruchsmöglichkeit

zu unterrichten. Die Unterrichtung kann auch in allgemeiner Form erfolgen, soweit eine Einzelunterrichtung wegen des damit verbundenen unverhältnismäßigen Aufwands nicht geboten erscheint und schutzwürdige Belange der Betroffenen nicht überwiegen.

§ 33
(aufgehoben)

Fünfter Abschnitt
Überwachung des Datenschutzes bei öffentlichen Stellen

§ 34
Sicherstellung des Datenschutzes

(1) Die Landesministerien, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen haben für ihren Bereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen.

(2) Der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf hinsichtlich der Datenarten und der regelmäßigen Datenübermittlung der vorherigen schriftlichen Freigabe durch die Stelle, die nach Absatz 1 den Datenschutz sicherzustellen hat. Entsprechendes gilt für wesentliche Änderungen der Verfahren.

(3) Automatisierte Verfahren,

1. die dem internen Verwaltungsablauf dienen, wie Registraturverfahren, ausschließlich der Erstellung von Texten dienende Verfahren sowie Kommunikations- und Anschriftenverzeichnisse zur Versendung an die Betroffenen,

2. die ausschließlich Zwecken der Datensicherung und Datenschutzkontrolle dienen und

3. deren einziger Zweck das Führen eines Registers ist, das aufgrund einer Rechtsvorschrift zur Information der Öffentlichkeit bestimmt ist,

bedürfen der Freigabe nicht. Einer Freigabe bedarf es ferner nicht, wenn das einzusetzende Verfahren unter Berücksichtigung der verarbeiteten oder genutzten Daten eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen nicht erwarten lässt. Die Ministerien regeln jeweils für ihren Geschäftsbereich und für die unter ihrer Aufsicht stehenden juristischen Personen des öffentlichen Rechts durch Rechtsverordnung, bei welchen Verfahren und Stellen die Voraussetzungen nach Satz 2 erfüllt sind.

(4) Sollen in einem Verfahren personenbezogene Daten aus verschiedenen Verwaltungszweigen verarbeitet werden, dann bedarf es der Zustimmung der beteiligten Stellen, die den Datenschutz sicherzustellen haben.

§ 35
Bestellung des Landesbeauftragten für den Datenschutz

(1) Der Landtag wählt auf Vorschlag der Landesregierung den Landesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Der Gewählte ist von der Landesregierung zu ernennen.

(2) Die Amtszeit des Landesbeauftragten für den Datenschutz beträgt sechs Jahre. Einmalige Wiederwahl ist zulässig.

(3) Der Präsident des Landtags verpflichtet den Landesbeauftragten für den Datenschutz vor dem Landtag, sein Amt gerecht und unparteiisch zu führen, das Grundgesetz und die Verfassung des Freistaats Thüringen sowie die Gesetze zu wahren und zu verteidigen. Der Landesbeauftragte für den Datenschutz leistet vor dem Präsidenten des Landtags folgenden Eid:

> "Ich schwöre, mein Amt gerecht und unparteiisch getreu dem Grundgesetz, der Verfassung des Freistaats Thüringen und den

Gesetzen zu führen und meine ganze Kraft dafür einzusetzen, so wahr mir Gott helfe."

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(4) Auf Vorschlag des Landesbeauftragten für den Datenschutz ernennt die Landesregierung einen Vertreter im Amt. Dieser soll die Befähigung zum Richteramt haben.

(5) Dienstsitz des Landesbeauftragten für den Datenschutz ist Erfurt.

(6) Die Landesregierung entlässt den Landesbeauftragten für den Datenschutz, wenn dieser es verlangt oder auf Vorschlag des Präsidenten des Landtags, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Bei Beendigung des Amtsverhältnisses erhält der Landesbeauftragte eine vom Ministerpräsidenten unterzeichnete Urkunde; die Entlassung wird mit der Aushändigung der Urkunde durch den Präsidenten des Landtags wirksam.

§ 36
Rechtsstellung und Verschwiegenheitspflicht

(1) Der Landesbeauftragte für den Datenschutz ist in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er steht zum Land nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis. Der Präsident des Landtags führt die Dienstaufsicht.

(2) Der Landesbeauftragte für den Datenschutz 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 Landesbeauftragte für den Datenschutz ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm bei seiner amtlichen Tätigkeit bekannt gewordenen 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.

(4) Der Landesbeauftragte für den Datenschutz ist oberste Dienstbehörde im Sinne von § 96 Strafprozeßordnung. Er trifft die Entscheidungen über Aussagegenehmigungen für sich und seine Mitarbeiter in eigener Verantwortung. Der Nachfolger im Amt entscheidet über die Aussagegenehmigung seiner Vorgänger.

(5) Dem Landesbeauftragten für den Datenschutz ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen. Für bestimmte Einzelfragen kann der Landesbeauftragte für den Datenschutz auch Dritte zur Mitarbeit heranziehen.

(6) Die Besetzung der Personalstellen erfolgt auf Vorschlag des Landesbeauftragten für den Datenschutz. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden; er ist ihr Dienstvorgesetzter, sie sind in ihrer Tätigkeit nach diesem Gesetz nur an seine Weisungen gebunden.

§ 36 a
Anwendung beamtenrechtlicher Vorschriften

(1) Der Landesbeauftragte für den Datenschutz erhält ab dem Tage seiner Ernennung bis zum Ablauf des Tages der Beendigung seines Amtsverhältnisses Amtsbezüge in Höhe der einem Landesbeamten bei einer obersten Landesbehörde der Besoldungsgruppe B 6 zustehenden Besoldung.

(2) Der Landesbeauftragte für den Datenschutz erhält Reisekosten, Umzugskosten, Trennungsgeld und Beihilfen nach den für die Landesbeamten geltenden Vorschriften. Gleiches gilt für die Unfallfürsorge und in Urlaubsangelegenheiten.

(3) Der Landesbeauftragte für den Datenschutz und seine Hinterbliebenen erhalten nach Beendigung seines Amtsverhältnisses Versorgung in entsprechender Anwendung der Bestimmungen des Besamtenversorgungsgesetzes für Beamte auf Zeit.

§ 37
Kontrolle durch den Landesbeauftragten für den Datenschutz

(1) Der Landesbeauftragte für den Datenschutz kontrolliert bei allen öffentlichen Stellen die Einhaltung der Bestimmungen dieses Gesetzes und anderer Rechtsvorschriften über den Datenschutz.

(2) Die Kontrolle des Landesbeauftragten für den Datenschutz erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Für personenbezogene Daten, die dem Arztgeheimnis unterliegen und personenbezogene Daten in Personalakten oder Akten über die Sicherheitsüberprüfung gilt dies

jedoch nur, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten nicht widersprochen hat. Unbeschadet des Kontrollrechts des Landesbeauftragten unterrichtet die Daten verarbeitende Stelle die Betroffenen in allgemeiner Form über das ihnen zustehende Widerspruchsrecht. Der Widerspruch ist schriftlich gegenüber der Daten verarbeitenden Stelle zu erklären.

(3) Die Kontrolle des Landesbeauftragten für den Datenschutz erstreckt sich nicht auf personenbezogene Daten, die der Kontrolle durch die Kommission nach § 3 des Landesgesetzes zur Ausführung des Bundesgesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 29. Oktober 1991 (GVBl. S. 515) in der jeweils geltenden Fassung unterliegen, es sei denn, die Kommission ersucht den Landesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

§ 38
Pflicht zur Unterstützung

(1) Der Landesbeauftragte für den Datenschutz und seine Beauftragten sind von allen öffentlichen Stellen in der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist im Rahmen der Kontrollbefugnis nach § 37 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 § 37 stehen,

2. jederzeit Zutritt in alle Diensträume zu gewähren.

(2) Für die in § 13 Abs. 3 genannten öffentlichen Stellen gilt Absatz 1

nur gegenüber dem Landesbeauftragten selbst und den von ihm schriftlich besonders damit Beauftragten. Absatz 1 Satz 2 findet für diese Stellen keine Anwendung, soweit das zuständige Landesministerium im Einzelfall feststellt, daß die Auskunft oder Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährden würde.

§ 39
Beanstandung durch den Landesbeauftragten für den Datenschutz

(1) Der Landesbeauftragte für den Datenschutz beanstandet festgestellte Verletzungen von Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten und fordert ihre Behebung in angemessener Frist. Die für die Sicherstellung des Datenschutzes nach § 34 verantwortliche Stelle und die Aufsichtsbehörde sind davon zu verständigen.

(2) Wird die Beanstandung nicht behoben, so fordert der Landesbeauftragte von der für die Sicherstellung des Datenschutzes nach § 34 verantwortlichen Stelle und der Aufsichtsbehörde binnen angemessener Frist geeignete Maßnahmen. Hat das nach Ablauf dieser Frist keinen Erfolg, verständigt der Landesbeauftragte den Landtag und die Landesregierung.

(3) Der Landesbeauftragte kann von einer Beanstandung absehen, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

§ 40
Weitere Aufgaben des Landesbeauftragten für den Datenschutz

(1) Der Landesbeauftragte für den Datenschutz erstattet dem Landtag und der Landesregierung mindestens alle zwei Jahre einen Bericht über seine Tätigkeit. Er gibt dabei auch einen Überblick über die technischen und organisatorischen Maßnahmen nach § 9 und regt Verbesserungen des Datenschutzes an.

(2) Der Ministerpräsident führt eine Stellungnahme der Landesregierung zu dem Bericht des Landesbeauftragten für den Datenschutz herbei und legt diese innerhalb von drei Monaten dem Landtag vor.

(3) Der Landesbeauftragte für den Datenschutz unterstützt im Rahmen seiner Beratungsaufgabe den Landtag bei seinen Entscheidungen. Auf Anforderung des Landtags oder der Landesregierung hat der Landesbeauftragte für den Datenschutz Gutachten zu erstellen und Berichte zu erstatten. Der Landtag oder die Landesregierung können den Landesbeauftragten ersuchen, bestimmte Vorgänge aus ihrem Aufgabenbereich zu überprüfen.

(4) Der Bericht nach Absatz 1 ist im Beirat beim Landesbeauftragten für den Datenschutz vorzuberaten.

(5) Der Landesbeauftragte für den Datenschutz beobachtet die Entwicklung und Nutzung der Informations- und Kommunikationstechnik, insbesondere der automatisierten Datenverarbeitung und ihre Auswirkungen auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen. Er hat insbesondere darauf zu achten, ob sie zu einer Verschiebung der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung und zwischen der staatlichen und der kommunalen Selbstverwaltung führen. Er soll Maßnahmen anregen, die ihm geeignet er-

scheinen, derartige Auswirkungen zu verhindern.

(6) Der Landesbeauftragte für den Datenschutz kann sich jederzeit an den Landtag wenden.

(7) Der Landesbeauftragte für den Datenschutz berät die in § 2 Abs. 1 und 2 genannten Stellen und gibt Empfehlungen zur Verbesserung des Datenschutzes.

§ 41
Beirat beim Landesbeauftragten für den Datenschutz

(1) Beim Landesbeauftragten für den Datenschutz wird ein Beirat gebildet. Er besteht aus neun Mitgliedern. Es bestellen sechs Mitglieder der Landtag, ein Mitglied die Landesregierung, ein Mitglied die kommunalen Spitzenverbände, ein Mitglied das Ministerium für Soziales und Gesundheit aus dem Bereich der gesetzlichen Sozialversicherungsträger. Für jedes Beiratsmitglied wird zugleich ein Stellvertreter bestellt.

(2) Die Mitglieder des Beirats werden für vier Jahre, die Mitglieder des Landtags für die Wahldauer des Landtags bestellt; sie sind in ihrer Tätigkeit an Aufträge und Weisungen nicht gebunden.

(3) Der Beirat unterstützt den Landesbeauftragten für den Datenschutz in seiner Arbeit. Die Unabhängigkeit des Landesbeauftragten für den Datenschutz nach § 36 Abs. 1 und die Berichtspflicht gegenüber dem Landtag werden dadurch nicht berührt.

(4) Der Beirat gibt sich eine Geschäftsordnung. Er tritt auf Antrag jedes seiner Mitglieder oder des Landesbeauftragten für den Datenschutz zusammen. Den Vorsitz führt ein Mitglied des Landtags.

(5) Der Landesbeauftragte für den Datenschutz nimmt an allen Sitzungen teil. Er verständigt den Beirat von Maßnahmen nach § 39 Abs. 1.

Vor Maßnahmen nach § 39 Abs. 2 kann dem Beirat Gelegenheit zur Stellungnahme gegeben werden.

(6) Die Mitglieder des Beirats haben, auch nach ihrem Ausscheiden, über die ihnen bei ihrer Tätigkeit bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Sechster Abschnitt
Aufsichtsbehörden für die Datenverarbeitung nichtöffentlicher Stellen

§ 42
Aufsichtsbehörde

(1) Die Aufsichtsbehörde nach § 38 Abs. 6 des Bundesdatenschutzgesetzes (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954, 2955) in der jeweils geltenden Fassung und der Landesbeauftragte für den Datenschutz tauschen regelmäßig die in Erfüllung ihrer Aufgaben gewonnenen Erfahrungen aus. Die Aufsichtsbehörde kann im Einzelfall mit Zustimmung des Landesbeauftragten für den Datenschutz Bedienstete der Geschäftsstelle des Landesbeauftragten für Datenschutz mit der Vornahme von Handlungen nach § 38 Abs. 3 und 4 BDSG beauftragen, sofern die Aufgaben des Landesbeauftragten für den Datenschutz dadurch nicht beeinträchtigt werden.

(2) Das für Angelegenheiten des Datenschutzes zuständige Ministerium wird ermächtigt, durch Rechtsverordnung sachverständige Personen oder Stellen zu bestimmen, derer sich die Aufsichtsbehörde zur Erfüllung ihrer Aufgaben nach § 38 BDSG bedienen kann. Eine Stelle nach Satz 1 nimmt insoweit hoheitlich Aufgaben der öffentlichen Verwaltung wahr. Die Bediensteten dieser Stelle haben die in § 38 Abs. 4 BDSG genannten Rechte; auch ihnen gegenüber besteht die in § 38 Abs. 3 BDSG genannte Auskunftspflicht.

(3) Das für Angelegenheiten des Datenschutzes zuständige Ministerium wird ermächtigt, durch Rechtsverordnung im Einvernehmen mit dem für Finanzen zuständigen Ministerium die Gebühren und Auslagen für die Tätigkeit der Aufsichtsbehörde nach § 38 Abs. 6 BDSG festzusetzen. Die Höhe der Gebühren und Auslagen ist nach dem Aufwand und der Bedeutung der Leistung für den Schuldner zu bemessen.

(4) In den Fällen, in denen das Bundesdatenschutzgesetz eine Meldepflicht gegenüber der Aufsichtsbehörde bestimmt, sind Gebühren und Auslagen von den Kontrollierten zu tragen. In den Fällen, in denen das Bundesdatenschutzgesetz keine Meldepflicht gegenüber der Aufsichtsbehörde bestimmt, sind Gebühren und Auslagen von den Kontrollierten zu tragen, wenn Mängel festgestellt werden. Werden keine Mängel festgestellt, sind Gebühren und Auslagen von denjenigen zu tragen, die die Tätigkeit veranlasst haben, soweit dies nicht der Billigkeit widerspricht. Für Unterstützungen des Beauftragten für den Datenschutz durch die für die Datenschutzkontrolle bei der Daten verarbeitenden Stelle zuständigen Behörde ist Schuldner die natürliche oder juristische Person, Gesellschaft oder andere Personenvereinigung des privaten Rechts, die den Beauftragten für den Datenschutz bestellt hat.

Siebter Abschnitt
Strafbestimmung, Übergangs- und Schlussbestimmungen

§ 43
Strafbestimmung

(1) Wer unbefugt personenbezogene Daten, die nicht offenkundig sind,

1. verarbeitet,
2. zum Abruf mittels automatisierten Verfahrens bereithält oder
3. abruft 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 nicht offenkundig sind, durch unrichtige Angaben erschleicht,
2. entgegen § 22 Abs. 4 Satz 1, § 24 Abs. 1 oder § 25 Abs. 1 die übermittelten Daten für einen anderen Zweck nutzt, indem er sie an Dritte weitergibt, oder
3. entgegen § 25 Abs. 3 Satz 3 die in § 25 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. Antragsberechtigt sind der Betroffene oder der Landesbeauftragte für den Datenschutz.

§ 43 a
Übergangsbestimmungen

(1) Das bislang beim Landesbeauftragten für den Datenschutz geführte Datenschutzregister ist innerhalb eines Jahres nach In-Kraft-Treten des Ersten Gesetzes zur Änderung des Thüringer Datenschutzgesetzes aufzulösen.

(2) Öffentliche Stellen im Sinne dieses Gesetzes haben innerhalb eines Jahres nach In-Kraft-Treten des Ersten Gesetzes zur Änderung des Thüringer Datenschutzgesetzes einen Beauftragten für den Datenschutz nach § 10 a zu bestellen.

§ 43 b
Gleichstellungsbestimmung

Status- und Funktionsbezeichnungen in diesem Gesetz gelten jeweils in männlicher und weiblicher Form.

§ 44
(In-Kraft-Treten)