

**Die Landesbeauftragte
für den Datenschutz und
für das Recht auf Akteneinsicht**



Brandenburgisches Datenschutzgesetz

**Brandenburgisches
Informationsgesetzbuch
Teil 1, Heft 1**

**Brandenburgisches Informationsgesetzbuch
Teil 1: Datenschutzgesetze
Heft 1**

Brandenburgisches Datenschutzgesetz

6., aktualisierte Auflage: Kleinmachnow, Juli 2010

Im Brandenburgischen Informationsgesetzbuch sind bisher erschienen:

Teil 1: Datenschutzgesetze

Heft 1 - Brandenburgisches Datenschutzgesetz

Heft 2 - Bundesdatenschutzgesetz

Teil 2: Informationszugangsgesetze

Heft 1 - Akteneinsichts- und Informationszugangsgesetz

Heft 2 - Umweltinformationsrecht

Heft 3 - Verbraucherinformationsrecht

Heft 4 - Informationsfreiheitsgesetz des Bundes

Impressum

Herausgeber: Die Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77, Haus 2
14532 Kleinmachnow

Telefon: 033203 356 - 0

Telefax: 033203 356 - 49

E-Mail: Poststelle@LDA.Brandenburg.de

Internet: <http://www.lda.brandenburg.de>

Fingerprint: 0DD7 0C8A 6550 8B73 2A53 EFEE AC85 7D66

Druck: Druckerei Pietsch, Kloster Lehnin

Stand: Juli 2010

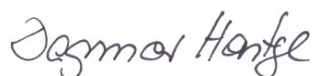
Einleitung

Das in Artikel 11 der Verfassung des Landes Brandenburg als Grundrecht verankerte Recht auf Datenschutz wird durch das Brandenburgische Datenschutzgesetz konkretisiert. Es gilt gegenüber den öffentlichen Stellen des Landes, den Landkreisen und den Gemeinden. Seine Vorschriften begrenzen die Verarbeitung personenbezogener Daten durch diese Stellen und dienen den Bürgerinnen und Bürgern somit als Maßstab für staatliches Handeln.

Seit seinem In-Kraft-Treten im Januar 1992 ist das Brandenburgische Datenschutzgesetz mehrfach geändert worden. Das Vierte Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes und anderer Rechtsvorschriften vom 25. Mai 2010 hat die Aufsicht über die Datenverarbeitung im Land Brandenburg zusammengeführt. Als Landesbeauftragte berate und kontrolliere ich seither sowohl öffentliche Stellen des Landes als auch Unternehmen mit Sitz in Brandenburg bei der Verarbeitung personenbezogener Daten. Meine Behörde ist zudem für die Verfolgung von Ordnungswidrigkeiten im Bereich des Datenschutzes zuständig.

Während die Rechte der Bürgerinnen und Bürger auf Datenschutz gegenüber öffentlichen Stellen des Landes durch das Brandenburgische Datenschutzgesetz geregelt werden, gilt gegenüber privaten Unternehmen das Bundesdatenschutzgesetz. Beide Gesetze bilden den Kern des von der Landesbeauftragten herausgegebenen Brandenburgischen Informationsgesetzbuches, das die wichtigsten informationsrechtlichen Regelungen enthält.

Bürgerinnen und Bürgern sowie Behörden und Unternehmen stehe ich für eine Beratung sowohl zu rechtlichen als auch zu technisch-organisatorischen Fragen des Datenschutzes jederzeit gerne zur Verfügung.



Dagmar Hartge
Landesbeauftragte für den Datenschutz
und für das Recht auf Akteneinsicht

**Gesetz zum Schutz personenbezogener
Daten im Land Brandenburg
(Brandenburgisches Datenschutzgesetz -
BbgDSG)**

in der Fassung vom 15. Mai 2008
(GVBl. I S. 114),
geändert durch Artikel 1 des Gesetzes
vom 25. Mai 2010
(GVBl. I Nr. 21)

Nicht amtliche Fassung

Inhaltsverzeichnis

**Abschnitt 1
Allgemeiner Datenschutz**

**Unterabschnitt 1
Allgemeine Bestimmungen**

- § 1 Aufgabe
- § 2 Anwendungsbereich
- § 3 Begriffsbestimmungen
- § 4 Zulässigkeit der Datenverarbeitung
- § 4a Verarbeitung besonderer Kategorien personenbezogener Daten
- § 4b Widerspruchsrecht des Betroffenen aus besonderem Grund
- § 5 Rechte des Betroffenen
- § 6 Datengeheimnis
- § 7 Sicherstellung des Datenschutzes
- § 7a Behördlicher Datenschutzbeauftragter
- § 8 Verfahrensverzeichnis
- § 9 Gemeinsame Verfahren, automatisierte Abrufverfahren und regelmäßige Datenübermittlungen
- § 10 Technische und organisatorische Maßnahmen
- § 10a Vorabkontrolle
- § 11 Verarbeitung personenbezogener Daten im Auftrag
- § 11a Wartung
- § 11b (aufgehoben)
- § 11c Datenschutzaudit

Unterabschnitt 2
Rechtsgrundlagen der Datenverarbeitung

- § 12 Erhebung
- § 13 Zweckbindung bei Speicherung, Veränderung und Nutzung
- § 14 Übermittlung innerhalb des öffentlichen Bereiches
- § 15 Übermittlung an öffentlich-rechtliche Religionsgesellschaften
- § 16 Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereiches
- § 17 Übermittlung an ausländische und internationale Stellen
- § 17a (aufgehoben)

Unterabschnitt 3
Rechte des Betroffenen

- § 18 Auskunft und Einsicht in Akten
- § 19 Berichtigung, Löschung und Sperrung
- § 20 Schadensersatz
- § 21 Anrufungsrecht des Betroffenen

Abschnitt 2
Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht

- § 22 Berufung und Rechtsstellung
- § 23 Aufgaben
- § 24 (aufgehoben)
- § 25 Beanstandungen durch den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht
- § 26 Durchführung der Kontrolle
- § 27 Tätigkeitsberichte und parlamentarische Kontrolle

**Abschnitt 3
Besonderer Datenschutz**

- § 28 Datenverarbeitung für wissenschaftliche Zwecke
- § 29 Datenverarbeitung bei Dienst- und Arbeitsverhältnissen
- § 30 Fernmessen und Fernwirken
- § 31 Verarbeitung personenbezogener Daten durch den Landtag
- § 32 (aufgehoben)
- § 33 Datenverarbeitung zu journalistisch-redaktionellen Zwecken
- § 33a Öffentliche Auszeichnungen und Ehrungen
- § 33b Begnadigungsverfahren
- § 33c Videoüberwachung und -aufzeichnung
- § 33d Mobile personenbezogene Speicher- und Verarbeitungsmedien
- § 34 (außer Kraft getreten)
- § 35 (außer Kraft getreten)
- § 36 (außer Kraft getreten)
- § 37 (außer Kraft getreten)

**Abschnitt 4
Straf- und Bußgeldvorschriften;
Übergangsvorschriften**

- § 38 Ordnungswidrigkeiten, Strafvorschrift
- § 39 (aufgehoben)
- § 40 Übergangsvorschriften
- § 40a Einschränkung von Grundrechten
- § 41 (Inkrafttreten)

Anlage 1 (aufgehoben)

Anlage 2 (aufgehoben)

Abschnitt 1
Allgemeiner Datenschutz

Unterabschnitt 1
Allgemeine Bestimmungen

§ 1
Aufgabe

Aufgabe dieses Gesetzes ist es, den einzelnen davor zu schützen, dass er durch die Verarbeitung personenbezogener Daten durch öffentliche Stellen in unzulässiger Weise in seinem Grundrecht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).

§ 2
Anwendungsbereich

(1) Dieses Gesetz gilt für die Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, die Gemeinden und Gemeindeverbände sowie für die sonstigen der Aufsicht des Landes oder der Gemeinden oder Gemeindeverbände unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen (öffentliche Stellen), soweit diese personenbezogene Daten verarbeiten. Für die Gerichte sowie für die Behörden der Staatsanwaltschaft gilt dieses Gesetz, soweit sie Verwaltungsaufgaben wahrnehmen; darüber hinaus gelten für die Behörden der Staatsanwaltschaft, soweit sie keine Verwaltungsaufgaben wahrnehmen nur die Vorschriften des Abschnittes 2 dieses Gesetzes. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben einer öffentlichen Stelle des Landes wahr, ist sie insoweit öffentliche Stelle im Sinne des Gesetzes.

(1a) Der Landtag, seine Gremien, seine Mitglieder, die Fraktionen sowie deren Verwaltungen und deren Beschäftigte unterliegen mit Ausnahme des § 31 nicht den Bestimmungen dieses Gesetzes, soweit sie zur Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten. Der Landtag erlässt insoweit unter Berücksichtigung seiner verfassungsrechtlichen Stellung und der Grundsätze dieses Gesetzes eine Datenschutzordnung.

(2) Von den Vorschriften dieses Gesetzes gelten die §§ 7a, 8, 10a, 21, 23 und 25 bis 30 dieses Gesetzes, soweit

1. wirtschaftliche Unternehmen der Gemeinden oder Gemeindeverbände ohne eigene Rechtspersönlichkeit (Eigenbetriebe),
2. öffentliche Einrichtungen, die entsprechend den Vorschriften über die Eigenbetriebe geführt werden,
3. Landesbetriebe,
4. der Aufsicht des Landes oder der Gemeinden oder Gemeindeverbänden unterstehende juristische Personen des öffentlichen Rechts, die am Wettbewerb teilnehmen,

personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. Im Übrigen sind mit Ausnahme der §§ 4d bis 4g und des § 38 die für nicht-öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anzuwenden.

(3) Die Vorschriften dieses Gesetzes gehen denen eines brandenburgischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden. Im Übrigen gehen besondere Rechtsvorschriften, die auf die Verarbeitung personenbezogener Daten anzuwenden sind, den Vorschriften dieses Gesetzes vor.

§ 3

Begriffsbestimmungen

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

(2) Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten. Im Einzelnen ist

1. Erheben (Erhebung) das Beschaffen von Daten über den Betroffenen,

2. Speichern (Speicherung) das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. Verändern (Veränderung) das inhaltliche Umgestalten gespeicherter Daten,
4. Übermitteln (Übermittlung) das Bekanntgeben von Daten an Dritte in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abrufen,
5. Sperren (Sperrung) das Verhindern weiterer Verarbeitung gespeicherter Daten,
6. Löschen (Löschung) das Unkenntlichmachen gespeicherter Daten,
7. Nutzen (Nutzung) jede sonstige Verwendung personenbezogener Daten,

ungeachtet der dabei verwendeten Verfahren.

(3) Im Sinne dieses Gesetzes ist

1. Anonymisieren 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 und
2. Pseudonymisieren das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen, um die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren,
3. Verschlüsseln das Ersetzen von Klartextbegriffen oder Zeichen durch andere in der Weise, dass der Klartext nur mit unverhältnismäßig großem Aufwand wieder lesbar gemacht werden kann,

4. ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ein Datenträger,
 - a) der zur Verfügung durch den Betroffenen bestimmt ist,
 - b) auf dem über die erstmalige Speicherung hinaus Daten automatisiert verarbeitet oder durch den Daten automatisiert verarbeitet werden können und
 - c) bei dem die Verarbeitung nach Buchstabe b durch andere als den Betroffenen erfolgt und der Betroffene dies nur durch den Gebrauch des Mediums beeinflussen kann.
 5. Wartung die Summe der Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen; dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie Überprüfung und Reparatur oder Austausch von Hardware und
 6. Fernwartung die Wartung der Soft- und Hardware von Datenverarbeitungsanlagen, die von einem Ort außerhalb der Stelle, bei der die Verarbeitung personenbezogener Daten erfolgt, mittels Einrichtungen zur Datenübertragung vorgenommen wird.
- (4) Im Sinne dieses Gesetzes ist
1. Daten verarbeitende Stelle jede öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt,
 2. Empfänger jede Person oder Stelle, die Daten erhält, und
 3. Dritter jede Stelle mit Ausnahme
 - a) der Daten verarbeitenden Stelle selbst,
 - b) des Betroffenen,
 - c) des Auftragnehmers in den Fällen der §§ 11 und 11a,

- d) der Personen, die unter der unmittelbaren Verantwortung der Daten verarbeitenden Stelle oder des Auftragnehmers nach Buchstabe c befugt sind, Daten zu verarbeiten.

(5) Automatisiert ist eine Datenverarbeitung, wenn sie durch Einsatz eines gesteuerten technischen Verfahrens selbsttätig ablaufen kann.

(6) Eine Datei ist eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder eine gleichartig aufgebaute Sammlung personenbezogener Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht-automatisierte Datei).

(7) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger, soweit sie nicht Dateien im Sinne von Absatz 6 sind; nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen und alsbald vernichtet werden.

§ 4

Zulässigkeit der Datenverarbeitung

(1) Personenbezogene Daten dürfen nur verarbeitet werden,

1. mit freiwilliger und ausdrücklicher Zustimmung (Einwilligung) des Betroffenen oder
2. soweit dies nach diesem Gesetz oder nach anderen Rechtsvorschriften zulässig ist.

(2) 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 der Betroffene auf die Einwilligungserklärung schriftlich besonders hinzuweisen. Der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung über die Empfänger der Daten sowie den Zweck der Übermittlung aufzuklären; er ist unter Darlegung der Rechtsfolgen

darauf hinzuweisen, dass er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann.

(3) Die Einwilligung kann auch elektronisch erklärt werden, wenn sichergestellt ist, dass

1. sie nur durch eine eindeutige und bewusste Handlung des Betroffenen erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. der Urheber erkannt werden kann,
4. die Einwilligung protokolliert wird und
5. die betroffene Person den Inhalt der Einwilligung jederzeit ohne unverhältnismäßigen Aufwand zur Kenntnis nehmen kann.

(4) Unzulässig ist eine zu rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen führende Entscheidung, wenn sie auf einer Bewertung einzelner Merkmale seiner Person beruht, die ausschließlich durch eine automatisierte Verarbeitung seiner Daten erstellt wurde. Eine Entscheidung nach Satz 1 kann durch Gesetz zugelassen werden, wenn es die Wahrung der berechtigten Interessen des Betroffenen sicherstellt.

(5) Sind personenbezogene Daten in Akten derart verbunden, dass ihre Trennung nach erforderlichen und nicht erforderlichen Daten auch durch Vervielfältigung und Unkenntlichmachung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so sind auch die Kenntnisnahme, die Weitergabe innerhalb der Daten verarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, zulässig, soweit nicht schutzwürdige Belange des Betroffenen oder eines Dritten überwiegen. Die nicht erforderlichen Daten unterliegen insoweit einem Verwertungsverbot.

§ 4a Verarbeitung besonderer Kategorien personenbezogener Daten

Soweit nicht andere Rechtsvorschriften die Verarbeitung personenbezogener Daten über die rassische und ethni-

sche Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben ausdrücklich vorsehen oder zwingend voraussetzen, ist diese nur zulässig,

1. mit Einwilligung des Betroffenen,
2. auf der Grundlage der §§ 15, 28, 29, 31, 33a, 33b und 33c oder
3. wenn sie zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist und der Betroffene aus rechtlichen oder tatsächlichen Gründen nicht in der Lage ist, seine Einwilligung zu geben.

Die Verarbeitung dieser Daten ist auch zulässig, wenn die Daten von dem Betroffenen offenkundig öffentlich gemacht wurden.

§ 4b

Widerspruchsrecht des Betroffenen aus besonderem Grund

Wenn der Betroffene schriftlich begründet, dass der rechtmäßigen Verarbeitung seiner Daten ein schutzwürdiges besonderes persönliches Interesse entgegensteht, ist die Verarbeitung der Daten nur zulässig, wenn im Einzelfall das öffentliche Interesse an der Datenverarbeitung gegenüber dem persönlichen Interesse des Betroffenen überwiegt. Dem Betroffenen ist das Ergebnis mit Begründung schriftlich mitzuteilen.

§ 5

Rechte des Betroffenen

(1) Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft über die zu seiner Person gespeicherten Daten sowie Einsicht in Akten (§ 18),
2. Gegenvorstellung aufgrund eines schutzwürdigen besonderen persönlichen Interesses (§ 4b),
3. Einsicht in das Verzeichnisse (§ 8 Abs. 4),

4. Berichtigung, Löschung oder Sperrung der zu seiner Person gespeicherten Daten (§ 19) und
5. Anrufung des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (§ 21 Abs. 1).

Auf diese Rechte kann der Betroffene nicht wirksam verzichten.

(2) Werden die Daten des Betroffenen in einem automatisierten Verfahren gespeichert, bei dem mehrere Stellen speicherberechtigt sind, kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Daten verarbeitende Stelle weiterzuleiten. Der Betroffene ist über die Weiterleitung und die Daten verarbeitende Stelle zu unterrichten. Die in § 19 Abs. 3 des Bundesdatenschutzgesetzes 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 Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht über die Weiterleitung und die Daten verarbeitende Stelle unterrichten. In diesem Fall richtet sich das weitere Vorgehen nach § 18 Absatz 6.

§ 6 Datengeheimnis

Denjenigen Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, solche Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder zu offenbaren. Diese Personen sind verpflichtet, das Datengeheimnis auch nach Beendigung ihrer Tätigkeit zu wahren.

§ 7 Sicherstellung des Datenschutzes

(1) Die obersten Landesbehörden, die Gemeinden und Gemeindeverbände sowie die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen haben jeweils für

ihren Bereich die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz sicherzustellen. Sie haben Verfahren zur Verarbeitung und Nutzung personenbezogener Daten an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten oder zu nutzen. Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist.

(2) Vor dem Erlass von Rechts- und Verwaltungsvorschriften, die die Verarbeitung personenbezogener Daten betreffen, ist der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht zu hören. Er ist über Planungen des Landes zum Aufbau oder zur wesentlichen Änderung automatisierter Informationssysteme rechtzeitig zu unterrichten, sofern in den Systemen personenbezogene Daten verarbeitet werden.

(3) Der erstmalige Einsatz oder die wesentliche Änderung von automatisierten Verfahren, für die ein Verfahrensverzeichnis nach § 8 zu erstellen ist, bedarf der schriftlichen Freigabe. Diese darf nur erteilt werden, wenn

1. ein aus einer Risikoanalyse entwickeltes Sicherheitskonzept ergeben hat, dass die von dem Verfahren ausgehenden Gefahren für die Rechte und Freiheiten der Betroffenen durch technisch-organisatorische Maßnahmen nach § 10 Abs. 1 und 2 beherrscht werden können und
2. in den Verfahren, in denen besondere Risiken für die Rechte und Freiheiten der Betroffenen ausgehen, eine Vorabkontrolle nach § 10a erfolgt ist.

Entsprechend der technischen Entwicklung ist die Ermittlung der zu treffenden technischen und organisatorischen Maßnahmen in angemessenen Abständen zu wiederholen. Die Freigabe erfolgt durch die Daten verarbeitende Stelle. Bei gemeinsamen Verfahren erfolgt die Freigabe für das gesamte Verfahren oder Teile des Verfahrens durch die von den beteiligten Stellen gemäß § 9 Absatz 1a Satz 1 bestimmten Stellen. Sie kann auch durch die zuständige ober-

ste Landesbehörde oder eine von ihr bestimmte Stelle erteilt werden.

§ 7a

Behördlicher Datenschutzbeauftragter

(1) Daten verarbeitende Stellen haben einen behördlichen Datenschutzbeauftragten zu bestellen. Bestellt werden darf nur, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt und wer dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird. Seine Bestellung kann gegen seinen Willen nur aus wichtigem Grund in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuches widerrufen werden.

(2) Die Daten verarbeitenden Stellen können einen Bediensteten einer anderen Daten verarbeitenden Stelle zum behördlichen Datenschutzbeauftragten bestellen.

(3) Der behördliche Datenschutzbeauftragte kann sich in dieser Funktion unmittelbar an die Leitung der Daten verarbeitenden Stelle wenden. Er ist in seiner Eigenschaft als behördlicher Datenschutzbeauftragter weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. In Zweifelsfällen kann sich der behördliche Datenschutzbeauftragte unmittelbar an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht wenden.

(4) Der behördliche Datenschutzbeauftragte 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) Der behördliche Datenschutzbeauftragte hat die Aufgabe, die Daten verarbeitende Stelle bei der Ausführung der Datenschutzvorschriften zu unterstützen. Zu seinen Aufgaben gehört es insbesondere,

1. auf die Einhaltung der Datenschutzvorschriften hinzuwirken,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen mit den Bestimmungen dieses Geset-

zes und anderer für die Daten verarbeitende Stelle einschlägigen Rechtsvorschriften vertraut zu machen,

3. die Daten verarbeitende Stelle bei der Umsetzung der nach § 7 Abs. 3 und nach den §§ 8, 10, 11, 11a und 26 erforderlichen Maßnahmen zu unterstützen und
4. die Vorabkontrolle nach § 10a vorzunehmen.

Er kann die zur Erfüllung seiner Aufgaben notwendige Einsicht in personenbezogene Datenverarbeitungsvorgänge nehmen. Berufs- oder besondere Amtsgeheimnisse können ihm nicht entgegengehalten werden.

§ 8

Verfahrensverzeichnis

(1) Für automatisierte Verarbeitungen personenbezogener Daten hat die Daten verarbeitende Stelle in einem Verzeichnis schriftlich oder elektronisch festzulegen:

1. die Bezeichnung des Verfahrens,
2. den Namen und die Anschrift der Daten verarbeitenden Stelle,
3. die Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung,
4. die betroffenen Personengruppen und die diesbezüglichen Daten oder Datenkategorien,
5. die Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden,
6. die geplanten Datenübermittlungen nach § 17 Abs. 2,
7. im Falle von § 11 die Auftragnehmer,
8. die Regelfristen für die Sperrung und Löschung der Daten,
9. die Beschreibung der Maßnahmen nach § 10,

10. die allgemeine Beschreibung der Art der eingesetzten Datenverarbeitungsanlagen und der verwendeten Software und

11. die Freigabeerklärung, gegebenenfalls das Ergebnis der Vorabkontrolle.

In den Fällen des § 7 Abs. 3 Satz 5 können die Festlegungen nach Satz 1 durch die zuständige oberste Landesbehörde oder die von ihr bestimmte Stelle getroffen werden.

(2) Das Führen des Verfahrensverzeichnisses ist dem behördlichen Datenschutzbeauftragten zu übertragen.

(3) Das Verfahrensverzeichnis ist bei wesentlichen Änderungen zu aktualisieren.

(4) Die Angaben des Verfahrensverzeichnisses gemäß Absatz 1 können von jedermann unentgeltlich eingesehen werden. Dies gilt nicht für Angaben nach Absatz 1 Nr. 7 bis 11, soweit hierdurch die Sicherheit des Verfahrens beeinträchtigt würde. Satz 1 gilt nicht für

1. Verfahren der Verfassungsschutzbehörde,
2. Verfahren, die der Gefahrenabwehr oder der Strafverfolgung dienen, und
3. Verfahren der Steuerfahndung,

soweit die Daten verarbeitende Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt.

(5) Absatz 1 gilt nicht für

1. Verfahren, deren einziger Zweck das Führen eines Registers ist, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht,
2. Verfahren, soweit mit ihnen Datensammlungen erstellt werden, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden,

3. Verfahren, die unter Einsatz handelsüblicher Schreibprogramme ablaufen,
4. Verfahren, die ausschließlich der Datensicherung und Datenschutzkontrolle dienen,
5. Verfahren, die ausschließlich dem Auffinden von Vorgängen, Anträgen oder Akten dienen (Registraturverfahren),
6. Verfahren, die ausschließlich zur Überwachung von Terminen und Fristen dienen,
7. Zimmer-, Inventar- und Softwareverzeichnisse,
8. Bibliothekskataloge und Fundstellenverzeichnisse oder
9. Anschriftenverzeichnisse, die ausschließlich für die Versendung von Informationen an Betroffene genutzt werden.

(6) Die Landesregierung wird ermächtigt, durch Rechtsverordnung das Nähere zur Ausgestaltung des Verfahrensverzeichnisses zu regeln, insbesondere zum Zweck der Vereinfachung des Verfahrens und zur Entlastung der Daten verarbeitenden Stelle.

§ 9

Gemeinsame Verfahren, automatisierte Abrufverfahren und regelmäßige Datenübermittlungen

(1) Die Einrichtung eines automatisierten Verfahrens, das mehreren Daten verarbeitenden Stellen die Verarbeitung personenbezogener Daten in oder aus einem gemeinsamen Datenbestand (gemeinsame Verfahren) oder die Übermittlung personenbezogener Daten an Dritte durch Abruf (automatisierte Abrufverfahren) ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist vorab zu unterrichten.

(1a) Vor der Einrichtung eines gemeinsamen Verfahrens bestimmen die beteiligten Stellen eine Stelle, der die Pla-

nung, Einrichtung und Durchführung des gemeinsamen Verfahrens obliegt, und legen schriftlich fest

1. die Bezeichnung und Aufgaben der beteiligten Stellen, einschließlich der Verantwortung für die Freigabe nach § 7 Absatz 3, sowie den Bereich der Verarbeitung, für deren Rechtmäßigkeit sie im Einzelfall verantwortlich sind, und
2. die für die Durchführung des gemeinsamen Verfahrens nach § 10 Absatz 2 zu treffenden technischen und organisatorischen Maßnahmen.

Die mit der Durchführung des gemeinsamen Verfahrens betraute Stelle verwahrt ein Doppel des von den beteiligten Stellen gemäß § 8 jeweils zu erstellenden Verfahrensverzeichnisses zusammen mit den Angaben nach Satz 1 Nummer 1. § 8 Absatz 4 gilt entsprechend.

(1b) Die Betroffenen können ihre Rechte nach § 5 Absatz 1 Nummer 1 bis 4 gegenüber jeder der an dem gemeinsamen Verfahren beteiligten Stellen geltend machen, unabhängig davon, welche Stelle im Einzelfall für die Verarbeitung der betroffenen Daten verantwortlich ist. Die Stelle, an die sich der Betroffene wendet, leitet das Anliegen an die jeweils zuständige Stelle weiter. Das Auskunftsrecht nach § 18 erstreckt sich auch auf die Angaben nach Absatz 1a Satz 1 Nummer 1.

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

1. den Anlass und Zweck des Abrufverfahrens,
2. die Empfänger der Daten,
3. die Art der zu übermittelnden Daten sowie
4. die nach § 10 erforderlichen technischen und organisatorischen Maßnahmen.

Die erforderlichen Festlegungen können auch durch die Fachaufsichtsbehörde getroffen werden.

(3) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Empfänger der Daten. Die übermittelnde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die übermittelnde Stelle überprüft die Übermittlung personenbezogener Daten durch geeignete Stichprobenverfahren.

(4) Für die Einrichtung automatisierter Abrufverfahren innerhalb einer öffentlichen Stelle gelten Absatz 1 Satz 1 und 2 sowie die Absätze 2 und 3 entsprechend.

(5) Die Absätze 1 bis 3 gelten nicht für Datenbestände, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

(6) Die Absätze 1 und 2 bis 5 sind auf die Zulassung regelmäßiger Datenübermittlungen entsprechend anzuwenden.

§ 10

Technische und organisatorische Maßnahmen

(1) Die Daten verarbeitenden Stellen oder die in ihrem Auftrag tätigen Stellen haben die technischen und organisatorischen Maßnahmen zu treffen, die nach den Absätzen 2 und 3 erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes zu gewährleisten. Die Maßnahmen haben für den angestrebten Schutzzweck angemessen zu sein und richten sich nach den im Einzelfall zu betrachtenden Risiken und dem jeweiligen Stand der Technik.

(2) Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

1. nur Befugte diese Daten zur Kenntnis nehmen können (Vertraulichkeit),
2. diese Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),
3. diese Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),

4. diese Daten jederzeit ihrem Ursprung zugeordnet werden können (Authentizität),
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit), und
6. die Verfahrensweisen bei der Verarbeitung dieser Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

(3) Werden personenbezogene Daten nicht-automatisiert oder in Akten verarbeitet, sind Maßnahmen zu treffen, um insbesondere den Zugriff Unbefugter bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung zu verhindern.

§ 10a Vorabkontrolle

(1) Die Verarbeitung personenbezogener Daten in automatisierten Verfahren, von denen besondere Risiken für die Rechte und Freiheiten der betroffenen Personen ausgehen, unterliegt der Prüfung (Vorabkontrolle) durch den behördlichen Datenschutzbeauftragten. Sie kann in den Fällen des § 7 Abs. 3 Satz 4 durch den behördlichen Datenschutzbeauftragten der zuständigen obersten Landesbehörde oder der von ihr bestimmten Stelle erfolgen.

(2) Eine Vorabkontrolle ist insbesondere durchzuführen, soweit

1. es sich um ein Verfahren nach § 9 Abs. 1 handelt oder mobile personenbezogene Speicher- und Verarbeitungsmedien eingesetzt werden oder
2. mit dem Verfahren personenbezogene Daten verarbeitet werden sollen, die zu einer in § 4a genannten Kategorien gehören oder einem Berufs- oder besonderen Amtsgeheimnis unterliegen.

(3) Dem behördlichen Datenschutzbeauftragten sind die zur Durchführung der Vorabkontrolle notwendigen Unterlagen, insbesondere die Ergebnisse der Risikoanalyse und das

Sicherheitskonzept sowie die Angaben für das Verzeichnisse nach § 8 zuzuleiten. Er hat im Zweifelsfall den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu konsultieren.

§ 11

Verarbeitung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag einer Daten verarbeitenden Stelle (Auftraggeber) durch andere Personen oder Stellen (Auftragnehmer) verarbeitet, bleibt die auftraggebende Stelle für die Einhaltung der Bestimmungen dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Rechte der Betroffenen sind ihr gegenüber geltend zu machen. Soweit die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, hat der Auftraggeber vertraglich sicherzustellen, dass der Auftragnehmer die Vorschriften dieses Gesetzes befolgt und jederzeit von ihm veranlasste Kontrollen ermöglicht.

(2) Der Auftrag ist unter Festlegung des Gegenstandes und des Umfanges der Datenverarbeitung, der technischen und organisatorischen Maßnahmen und etwaiger Unterauftragsverhältnisse schriftlich zu erteilen. Der Auftragnehmer muss Gewähr für die Einhaltung der technischen und organisatorischen Maßnahmen nach § 10 bieten. Werden Daten im Auftrag verarbeitet, für die gesetzliche oder andere Geheimhaltungspflichten bestehen, sind besondere technische und organisatorische Maßnahmen zu treffen, die eine Wahrung der Geheimnisse sicherstellen. Der Auftrag kann auch durch die Fachaufsichtsbehörde mit Wirkung für die ihrer Aufsicht unterliegenden öffentlichen Stellen des Landes erteilt werden; diese sind hiervon zu unterrichten.

(3) Der Auftragnehmer darf die personenbezogenen Daten nur im Rahmen der Weisungen der auftraggebenden Stelle verarbeiten.

(4) Ist der Auftragnehmer eine in § 2 Abs. 1 Satz 1 oder 2 genannte Stelle, gelten für ihn neben Absatz 3 nur die §§ 6, 7a, 10 und 11a sowie 21, 23, 25, 26 und 38.

(5) Zur Durchführung von beratenden oder begutachtenden Tätigkeiten im Auftrag der Daten verarbeitenden Stelle ist die Übermittlung personenbezogener Daten zulässig,

wenn die übermittelnde Stelle die beauftragten Personen verpflichtet,

1. die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihnen überlassen worden sind, und
2. nach Erledigung des Auftrags die ihnen überlassenen Datenträger zurückzugeben und die bei ihnen gespeicherten Daten zu löschen, soweit nicht besondere Rechtsvorschriften entgegenstehen.

Die Absätze 1 bis 3 gelten entsprechend.

§ 11a Wartung

(1) Datenverarbeitungssysteme sind so zu gestalten, dass bei ihrer Wartung möglichst nicht auf personenbezogene Daten zugegriffen werden kann. Sofern dies nicht sichergestellt ist, hat die Daten verarbeitende Stelle durch technische und organisatorische Maßnahmen sicherzustellen, dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann.

(2) Eine Wartung durch andere Stellen darf über die Anforderungen nach Absatz 1 hinaus nur aufgrund schriftlicher Vereinbarungen erfolgen. Es gilt § 11 Absatz 2 Satz 1 und 2 entsprechend. Die mit Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

(3) Ist bei Wartungsarbeiten nur ein Zugriff auf Daten in verschlüsselter, pseudonymisierter oder anonymisierter Form gegeben, so dass die mit der Wartung betraute Stelle Betroffene nicht reidentifizieren kann, sind nur Maßnahmen nach Absatz 2 Satz 1 und 3 erforderlich.

§ 11b (aufgehoben)

§ 11c Datenschutzaudit

Die öffentlichen Stellen können zur Verbesserung von Datenschutz und Datensicherheit sowie zum Erreichen größt-

möglicher Datensparsamkeit ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Sie können auch bereits geprüfte und bewertete Datenschutzkonzepte und -programme zum Einsatz bringen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

Unterabschnitt 2 Rechtsgrundlagen der Datenverarbeitung

§ 12 Erhebung

(1) Das Erheben personenbezogener Daten ist nur zulässig, wenn ihre Kenntnis zur rechtmäßigen Erfüllung der durch Gesetz der erhebenden Stelle zugewiesenen Aufgabe und für den jeweils damit verbundenen Zweck erforderlich ist.

(2) Personenbezogene Daten sind grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. In diesem Falle ist er über den Verwendungszweck aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Werden die Daten aufgrund einer Rechtsvorschrift erhoben, so ist der Betroffene in geeigneter Weise über diese aufzuklären. Soweit eine Auskunftspflicht besteht oder die Angaben die Voraussetzung für die Gewährung von Rechtsvorteilen sind, ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben, hinzuweisen.

(3) Personenbezogene Daten dürfen ohne Kenntnis des Betroffenen bei anderen Stellen oder Personen unter den Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstabe a und c bis f erhoben werden. Beim Betroffenen dürfen Daten ohne seine Kenntnis nur erhoben werden, wenn eine Rechtsvorschrift dies vorsieht oder, soweit es sich um eine Rechtsvorschrift des Bundes handelt, zwingend voraussetzt oder der Schutz von Leben oder Gesundheit oder die Abwehr einer erheblichen Gefährdung der natürlichen Lebensgrundlagen dies erforderlich macht.

(4) Werden Daten bei einer dritten Person oder einer nicht-öffentlichen Stelle erhoben, so ist diese auf Verlangen über den Verwendungszweck aufzuklären. Soweit eine Auskunftspflicht besteht, ist sie hierauf, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(5) Werden Daten ohne Kenntnis des Betroffenen erhoben, ist er davon zu benachrichtigen, sobald die rechtmäßige Erfüllung der Aufgabe dadurch nicht mehr gefährdet wird. Absatz 2 Satz 1 und 2 gilt entsprechend. Werden die Daten nicht beim Betroffenen erhoben, kann von einer Benachrichtigung abgesehen werden, wenn

1. durch Gesetz ausdrücklich bestimmt ist, dass die Daten bei anderen Stellen oder Personen erhoben werden,
2. der Betroffene auf andere Weise Kenntnis von der Verarbeitung erlangt hat oder
3. sie unmöglich ist oder einen unverhältnismäßigen Aufwand erfordern würde.

§ 13 Zweckbindung bei Speicherung, Veränderung und Nutzung

(1) Das Speichern, Verändern und Nutzen personenbezogener Daten ist zulässig, wenn es zur rechtmäßigen Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist. Die Daten dürfen nur für Zwecke gespeichert, verändert oder genutzt werden, für die sie erhoben worden sind. Daten, von denen die Stelle ohne Erhebung Kenntnis erlangt hat, dürfen nur für Zwecke genutzt und verändert werden, für die sie erstmals gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken gespeichert, verändert oder genutzt werden, für die sie nicht erhoben oder erstmals gespeichert worden sind, ist dies nur zulässig, wenn

- a) eine Rechtsvorschrift dies erlaubt oder die Wahrnehmung einer durch Gesetz oder Rechtsverordnung zugewiesenen einzelnen Aufgabe die Verarbeitung dieser Daten zwingend voraussetzt,

- b) der Betroffene eingewilligt hat,
- c) die Bearbeitung eines vom Betroffenen gestellten Antrages ohne diese Zweckänderung der Daten nicht möglich ist oder es erforderlich ist, Angaben des Betroffenen zu überprüfen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
- d) es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,
- e) die Einholung der Einwilligung des Betroffenen nicht möglich ist oder mit unverhältnismäßig hohem Aufwand verbunden wäre, aber offensichtlich ist, dass es in seinem Interesse liegt und er in Kenntnis des anderen Zweckes seine Einwilligung erteilen würde,
- f) sie aus allgemein zugänglichen Quellen entnommen werden können oder die Daten verarbeitende Stelle sie veröffentlichen dürfte, es sei denn, dass das Interesse des Betroffenen an dem Ausschluss der Speicherung oder einer Veröffentlichung der gespeicherten Daten offensichtlich überwiegt, oder
- g) sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheint.

Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der Daten verarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, findet Satz 1 Buchstabe c bis g keine Anwendung.

(3) Eine Verarbeitung zu anderen Zwecken liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient. Der Zugriff auf personenbezogene Daten ist insoweit nur zulässig, als er für die Ausübung dieser Befugnisse unverzichtbar ist. Zu Aus-

und Fortbildungszwecken dürfen personenbezogene Daten nur verwendet werden, wenn dies unerlässlich ist und schutzwürdige Belange des Betroffenen dem nicht entgegenstehen; zu Test- und Prüfungszwecken dürfen personenbezogene Daten nicht verwendet werden.

§ 14

Übermittlung innerhalb des öffentlichen Bereiches

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und die Voraussetzungen des § 13 Abs. 1 Satz 2 oder 3 oder des Absatzes 2 Satz 1 vorliegen, sowie zur Wahrnehmung von Aufgaben nach § 13 Abs. 3. Die Übermittlung ist ferner zulässig, soweit es zur Entscheidung in einem Verwaltungsverfahren der Beteiligung mehrerer öffentlicher Stellen bedarf.

(2) (gestrichen)

(3) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung aufgrund eines Ersuchens des Empfängers, hat die übermittelnde Stelle lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt. Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht; der Empfänger hat der übermittelnden Stelle die für diese Prüfung erforderlichen Angaben zu machen. Erfolgt die Übermittlung durch automatisierten Abruf (§ 9), so trägt die Verantwortung für die Rechtmäßigkeit des Abrufes der Empfänger.

(4) Der Empfänger darf die übermittelten Daten nur für die Zwecke verarbeiten, zu deren Erfüllung sie ihm übermittelt worden sind; § 13 Abs. 2 findet entsprechende Anwendung.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 15
Übermittlung an öffentlich-rechtliche
Religionsgemeinschaften

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgemeinschaften ist in entsprechender Anwendung der Vorschriften über die Datenübermittlung an öffentliche Stellen zulässig, sofern sichergestellt ist, dass bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen sind.

§ 16
Übermittlung an Personen oder Stellen außerhalb
des öffentlichen Bereiches

(1) Die Übermittlung personenbezogener Daten an Stellen nach § 2 Abs. 2 Satz 1, soweit sie die Daten für die Verfolgung ihrer wirtschaftlichen Zwecke oder Ziele benötigen, sowie an Personen oder Stellen außerhalb des öffentlichen Bereiches, ist zulässig, wenn

- a) sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen des § 13 Abs. 1 vorliegen,
- b) die Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstabe a, b, d oder f vorliegen,
- c) der Auskunftsbeghernde ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und kein Grund zu der Annahme besteht, dass das Geheimhaltungsinteresse des Betroffenen überwiegt, oder
- d) sie im öffentlichen Interesse liegt oder hierfür ein berechtigtes Interesse geltend gemacht wird und der Betroffene in diesen Fällen der Datenübermittlung nicht widersprochen hat.

(2) In den Fällen des Absatzes 1 Buchstabe d ist der Betroffene über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise zu unterrichten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt.

(3) Der Empfänger darf die übermittelten Daten nur für die Zwecke verarbeiten, zu denen sie ihm übermittelt wurden.

(4) Die übermittelnde Stelle kann die Datenübermittlung mit Auflagen versehen, die den Datenschutz beim Empfänger sicherstellen.

§ 17 Übermittlung an ausländische und internationale Stellen

(1) Die Zulässigkeit der Übermittlung personenbezogener Daten an Stellen in anderen Mitgliedstaaten der Europäischen Union, in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder der Organe und Einrichtungen der Union richtet sich nach § 4.

(2) Für die Übermittlung personenbezogener Daten an andere als die in Absatz 1 genannten Stellen sowie an über- und zwischenstaatliche Stellen ist § 16 Abs. 1, 2 und 4 nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen nur dann anzuwenden, wenn diese Stellen ein angemessenes Datenschutzniveau gewährleisten.

(3) Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die in den Stellen nach Absatz 2 geltenden Rechtsnormen sowie die dort geltenden Landesregeln und Sicherheitsmaßnahmen herangezogen werden.

(4) Sofern Stellen nach Absatz 2 kein angemessenes Datenschutzniveau gewährleisten, ist eine Übermittlung personenbezogener Daten nur zulässig, sofern

1. der Betroffene eingewilligt hat,
2. die Übermittlung für die Erfüllung eines Vertrages zwischen der übermittelnden Stelle und dem Betroffenen oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,

3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrages erforderlich ist, der im Interesse des Betroffenen mit einem Dritten geschlossen wurde oder geschlossen werden soll,
4. die Übermittlung zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung eines rechtlichen Interesses erforderlich ist,
5. die Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist,
6. die Übermittlung aus einem für die Öffentlichkeit bestimmten Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind oder
7. die empfangende Stelle ausreichende Garantien hinsichtlich des Schutzes der Grundrechte bietet.

(5) Datenübermittlungen nach Absatz 4 Nr. 7 sind dem für Inneres zuständigen Mitglied der Landesregierung mitzuteilen.

(6) Die Stelle, der die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu Zwecken verarbeitet werden dürfen, die mit den Zwecken vereinbar sind, zu deren Erfüllung sie ihr übermittelt werden.

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

**§ 17a
(aufgehoben)**

**Unterabschnitt 3
Rechte des Betroffenen**

**§ 18
Auskunft und Einsicht in Akten**

(1) Dem Betroffenen ist von der Daten verarbeitenden Stelle auf Antrag Auskunft zu erteilen über:

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. die Herkunft der Daten und Empfänger übermittelter Daten, soweit diese gespeichert sind,
4. die Empfänger regelmäßiger Datenübermittlungen und
5. den logischen Aufbau der automatisierten Verarbeitung im Falle einer automatisierten Entscheidung gemäß § 4 Abs. 4.

Dies gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen.

(2) Die Daten verarbeitende Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen; sind die Daten in Akten oder nicht-automatisiert gespeichert, ist dem Betroffenen auf Verlangen Einsicht zu gewähren. Die Akteneinsicht ist auf die Teile der Akten beschränkt, die personenbezogene Daten des Betroffenen enthalten, soweit sich aus einem Verwaltungsverfahrensgesetz nichts anderes ergibt. Auskunft aus Akten oder Akteneinsicht sind zu gewähren, soweit der Betroffene Angaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglichen. Auskunftserteilung und Akteneinsicht sind gebührenfrei; Erstattung von Auslagen kann verlangt werden.

(3) Die Verpflichtung zur Auskunftserteilung oder zur Gewährung der Akteneinsicht entfällt, soweit die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden be-

rechtigten Interessen eines Dritten geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(4) Einer Begründung für die Auskunftsverweigerung bedarf es nur dann nicht, wenn durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall sind die wesentlichen Gründe für die Entscheidung aufzuzeichnen.

(5) Bezieht sich die Auskunftserteilung oder die Akteneinsicht auf die Herkunft personenbezogener Daten von Behörden des Verfassungsschutzes, der Staatsanwaltschaft und der Polizei, von Landesfinanzbehörden, soweit diese personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, sowie von den in § 19 Abs. 3 des Bundesdatenschutzgesetzes genannten Behörden, ist sie nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt für die Übermittlung personenbezogener Daten an diese Behörden. Für die Versagung der Zustimmung gelten, soweit dieses Gesetz auf die genannten Behörden Anwendung findet, die Absätze 5 und 6 entsprechend.

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

§ 19

Berichtigung, Löschung und Sperrung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Sind personenbezogene Daten, die nicht-automatisiert verarbeitet werden, oder in Akten zu berichtigen, so ist in geeigneter Weise kenntlich zu machen, zu welchem Zeitpunkt und aus welchem Grund diese Daten unrichtig waren oder geworden sind.

(2) Personenbezogene Daten sind zu löschen, wenn

- a) ihre Speicherung unzulässig ist oder
- b) ihre Kenntnis für die Daten verarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Sind personenbezogene Daten in Akten gespeichert, ist die Löschung nach Satz 1 Buchstabe b nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist, es sei denn, dass der Betroffene die Löschung verlangt und die weitere Speicherung ihn in unangemessener Weise beeinträchtigen würde. Soweit hiernach eine Löschung nicht in Betracht kommt, sind die personenbezogenen Daten auf Antrag des Betroffenen zu sperren.

(3) An die Stelle einer Löschung tritt eine Sperrung der personenbezogenen Daten, wenn

- a) ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt,
- b) der Betroffene an Stelle der Löschung nach Absatz 2 Satz 1 Buchstabe a die Sperrung verlangt,
- c) die weitere Speicherung im Interesse des Betroffenen geboten ist,
- d) sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind oder
- e) die Voraussetzungen des Absatzes 2 Satz 1 Buchstabe b vorliegen und die Daten aber aufgrund gesetzlicher Aufbewahrungsfristen nicht gelöscht werden dürfen.

In den Fällen nach Satz 1 Buchstabe c sind die Gründe aufzuzeichnen. Bei automatisiert verarbeiteten Daten ist die Sperrung grundsätzlich durch technische Maßnahmen sicherzustellen; im Übrigen ist ein entsprechender Vermerk anzubringen. Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur verarbeitet werden, wenn dies zu wissenschaftlichen Zwecken, zur Behebung einer Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich oder zur Wahrnehmung von Aufsichts- oder Kon-

trollbefugnissen oder zur Rechnungsprüfung erforderlich ist und die Daten hierfür verarbeitet werden könnten, wenn sie nicht gesperrt wären.

(4) Abgesehen von den Fällen des Absatzes 2 Satz 1 Buchstabe a ist von einer Löschung abzusehen, soweit die gespeicherten Daten aufgrund des Brandenburgischen Archivgesetzes dem zuständigen öffentlichen Archiv zur Übernahme anzubieten sind und von diesem übernommen werden.

(5) Über die Berichtigung unrichtiger Daten, die Sperrung bestrittener Daten und die Löschung oder Sperrung unzulässig gespeicherter Daten sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt worden sind. Die Unterrichtung kann unterbleiben, wenn sie einen erheblichen Aufwand erfordern würde und nachteilige Folgen für den Betroffenen nicht zu befürchten sind. Die Sätze 1 und 2 gelten entsprechend, wenn Daten innerhalb einer öffentlichen Stelle weitergegeben wurden.

§ 20 Schadenersatz

(1) Entsteht dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten in oder aus Dateien ein Vermögensnachteil, ist die Daten verarbeitende Stelle oder deren Träger zum Ersatz verpflichtet. In schweren Fällen kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Eine Schadenersatzpflicht besteht nicht, soweit die Daten verarbeitende Stelle den Umstand, durch den der Schaden eingetreten ist, nicht zu vertreten hat. Der Nachweis obliegt der Daten verarbeitenden Stelle oder deren Träger. Gegenüber dem Betroffenen hat die Daten verarbeitende Stelle auch diejenigen Umstände zu vertreten, für die in den Fällen der §§ 11 und 11a der Auftragnehmer verantwortlich ist. Der Anspruch ist insgesamt auf eine Höhe von 125 000 Euro begrenzt.

(2) Auf eine schuldhafte Mitverursachung des Schadens durch den Betroffenen und die Verjährung des Schadensanspruches sind die §§ 254, 839 Abs. 3 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(3) Weitergehende sonstige Schadenersatzansprüche bleiben unberührt.

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

§ 21

Anrufungsrecht des Betroffenen

(1) Jedermann hat das Recht, sich unmittelbar an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine der Kontrolle des Landesbeauftragten unterliegende Stelle in seinen Rechten verletzt zu sein; dies gilt auch für Bedienstete der öffentlichen Stellen, ohne dass der Dienstweg einzuhalten ist.

(2) Niemand darf deswegen benachteiligt oder gemäßregelt werden, weil er sich an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht wendet.

Abschnitt 2

Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht

§ 22

Berufung und Rechtsstellung

(1) Der Landtag wählt einen Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Dieser muss die Befähigung zum Richteramt oder zum höheren Dienst oder eine nach dem Einigungsvertrag gleichgestellte Befähigung haben und die zur Erfüllung seiner Aufgaben erforderliche Fachkunde besitzen.

(2) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht leistet vor dem Präsidenten des Landtages folgenden Eid:

"Ich schwöre, mein Amt gerecht und unparteiisch getreu dem Grundgesetz, der Verfassung von Brande-

burg und den Gesetzen zu führen und meine ganze Kraft dafür einzusetzen."

Der Eid kann auch mit einer religiösen Beteuerung geleistet werden.

(3) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht wird jeweils auf die Dauer von sechs Jahren in ein Beamtenverhältnis auf Zeit berufen. Die Wiederwahl ist zulässig. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht führt das Amt bis zur Bestellung eines Nachfolgers, längstens jedoch für sechs Monate nach Ablauf seiner Amtszeit, fort. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht kann außer auf eigenen Antrag nur entlassen werden, wenn er der Pflicht nach Satz 3 nicht nachkommt oder wenn Gründe vorliegen, die bei einem Richterverhältnis auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen.

(4) Das Amt des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht wird bei dem Präsidenten des brandenburgischen Landtages eingerichtet. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Dienstaufsicht des Präsidenten des Landtages. Für die Erfüllung der Aufgaben ist die notwendige Personal- und Sachausstattung zur Verfügung zu stellen, die Mittel sind im Einzelplan des Landtages in einem gesonderten Kapitel auszuweisen. Die Mitarbeiter werden auf Vorschlag des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht durch den Präsidenten des Landtages ernannt. Sie können nur im Einvernehmen mit dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht versetzt oder abgeordnet werden. Ihr Dienstvorgesetzter ist der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht, an dessen Weisungen sie ausschließlich gebunden sind. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht bestellt einen Mitarbeiter zum Stellvertreter. Dieser führt die Geschäfte, wenn der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht an der Ausübung des Amtes verhindert ist.

(5) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist oberste Dienstbehörde im Sin-

ne von § 96 der Strafprozessordnung. Er trifft die Entscheidungen über Aussagegenehmigungen für sich und seine Mitarbeiter in eigener Verantwortung.

(6) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht 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.

(7) Der Landesbeauftragte für den Datenschutz übt zugleich die Aufgaben eines Landesbeauftragten für das Recht auf Akteneinsicht gemäß den Vorschriften des Akteneinsichts- und Informationszugangsgesetzes aus. Seine Amts- und Funktionsbezeichnung lautet "Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht"; diese kann in männlicher und weiblicher Form geführt werden.

§ 23 Aufgaben

(1) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht kontrolliert die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz sowie die Einhaltung des Akteneinsichts- und Informationszugangsgesetzes gemäß § 11 Absatz 2 des Akteneinsichts- und Informationszugangsgesetzes bei den Behörden und sonstigen öffentlichen Stellen soweit nach § 2 der Anwendungsbereich dieses Gesetzes eröffnet ist oder sich Daten verarbeitende Stellen gemäß § 11 Absatz 1 Satz 3 seiner Kontrolle unterworfen haben.

(1a) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist auch Aufsichtsbehörde nach § 38 des Bundesdatenschutzgesetzes für die Datenverarbeitung nicht-öffentlicher Stellen.

(2) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht kann Empfehlungen zur Verbesserung des Datenschutzes geben. Insbesondere kann er die Landesregierung und einzelne Minister, die Gemeinden und Gemeindeverbände sowie die übrigen öffentlichen Stellen in Fragen des Datenschutzes beraten.

(3) Auf Ersuchen des Landtages, des Petitionsausschusses oder des Ausschusses für Inneres oder der Landesregierung geht der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ferner Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenbereich unmittelbar betreffen, nach. Er geht außerdem Hinweisen nach, die sich aus der Wahrnehmung des Rechts des Betroffenen nach § 21 ergeben.

(4) Der Landtag und die Landesregierung können den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht mit der Erstattung von Gutachten und Stellungnahmen oder der Durchführung von Untersuchungen in Datenschutzfragen betrauen. § 22 Abs. 4 Satz 2 bleibt unberührt.

(5) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht kann nach Maßgabe der Geschäftsordnung des Landtages an den Sitzungen des Landtages und seiner Ausschüsse teilnehmen und Stellung nehmen zu Fragen, die für den Datenschutz von Bedeutung sind. Der Landtag und seine Ausschüsse können seine Anwesenheit und seine mündliche oder schriftliche Stellungnahme verlangen.

(6) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist berechtigt, die für die Erfüllung seiner ihm durch dieses Gesetz zugewiesenen Aufgaben erforderlichen personenbezogenen Daten unter den Voraussetzungen dieses Gesetzes zu verarbeiten. Er darf personenbezogene Daten im Rahmen von Kontrollmaßnahmen im Einzelfall auch ohne Kenntnis der Betroffenen erheben, wenn nur auf diese Weise festgestellt werden kann, ob ein datenschutzrechtlicher Mangel besteht. Die nach den Sätzen 1 und 2 verarbeiteten Daten dürfen nicht zu anderen Zwecken gespeichert, verändert oder genutzt werden.

(7) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht arbeitet mit den Behörden und sonstigen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 des Bundesdatenschutzgesetzes zusammen. Er ist berechtigt, für diese Stellen auf ihr Ersuchen die Einhaltung datenschutzrechtlicher Vorschriften zu kontrollieren und zu diesem Zweck personenbezogene Daten zu verarbeiten; das gleiche gilt, wenn sich eine nicht-öffentliche

Stelle durch einen Vertrag im Sinne des § 11 Abs. 1 Satz 3 seiner Kontrolle unterworfen hat.

(8) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist zuständige Behörde für die Verfolgung von Ordnungswidrigkeiten nach § 38 dieses Gesetzes, § 43 des Bundesdatenschutzgesetzes sowie anderer datenschutzrechtlicher Regelungen. Er ist auch hilfeleistende Behörde nach Artikel 13 Nummer 2 Buchstabe a des Übereinkommens vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

**§ 24
(aufgehoben)**

**§ 25
Beanstandungen durch den Landesbeauftragten für
den Datenschutz und für das Recht auf Akteneinsicht**

(1) Stellt der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Verstöße gegen die Vorschriften dieses Gesetzes, gegen andere Vorschriften über den Datenschutz, sonstige Mängel bei der Verarbeitung personenbezogener Daten oder Verstöße gegen das Akteneinsichts- und Informationszugangsgesetz fest, so beanstandet er diese

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,
2. bei der Kommunalverwaltung gegenüber der jeweils verantwortlichen Gemeinde oder dem verantwortlichen Gemeindeverband,
3. bei den wissenschaftlichen Hochschulen und Fachhochschulen gegenüber dem Hochschulpräsidenten oder dem Rektor, bei öffentlichen Schulen gegenüber dem Leiter der Schule,
4. bei den sonstigen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts 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. 2 bis

4 unterrichtet der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht gleichzeitig auch die zuständige Aufsichtsbehörde.

(2) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt oder wenn ihre Behebung sichergestellt ist.

(3) Mit der Beanstandung kann der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die gemäß Absatz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht getroffen worden sind. Die in Absatz 1 Nr. 2 bis 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu.

(5) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist nach pflichtgemäßem Ermessen befugt, Betroffene über Beanstandungen und die hierauf erfolgten Maßnahmen nach Absatz 4 zu unterrichten.

§ 26

Durchführung der Kontrolle

(1) Die öffentlichen Stellen sind verpflichtet, den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist insbesondere

1. Auskunft auf ihre Fragen zu erteilen sowie Einsicht in alle Vorgänge und Aufzeichnungen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,
2. jederzeit Zutritt zu allen Diensträumen zu gewähren.

Die Einsicht nach Nummer 1 kann auch elektronisch gewährt werden.

(2) Absatz 1 gilt für die in § 18 Absatz 5 genannten Behörden nicht, soweit das jeweils zuständige Mitglied der Landesregierung im Einzelfall feststellt, dass die Einsicht in die Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet. Auf Antrag des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht hat die Landesregierung dies im zuständigen Ausschuss des Landtages in geheimer Sitzung zu begründen. Die Entscheidung des Ausschusses kann veröffentlicht werden.

(3) Berufs- und Amtsgeheimnisse entbinden nicht von der Unterstützungspflicht.

§ 27

Tätigkeitsberichte und parlamentarische Kontrolle

(1) Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht legt dem Landtag und der Landesregierung alle zwei Jahre einen Bericht über seine Tätigkeit nach § 23 Absatz 1 vor. Die Landesregierung legt hierzu regelmäßig innerhalb von vier Monaten nach Vorlage des Tätigkeitsberichtes dem Landtag ihre Stellungnahme vor. Gleichzeitig legt der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht dem Landtag einen Bericht über seine Tätigkeit nach § 23 Absatz 1a vor.

(2) Jeder Abgeordnete hat das Recht, Anfragen an den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu stellen, von ihm Auskunft zu verlangen oder Einsicht in Akten und sonstige amtliche Unterlagen zu nehmen. Anfragen sind unverzüglich nach bestem Wissen und vollständig zu beantworten. Das Nähere regelt die Geschäftsordnung des Landtages. Das Auskunftsverlangen oder die Einsichtnahme darf abgelehnt werden, soweit überwiegende öffentliche oder überwiegende private Interessen an der Geheimhaltung dies zwingend erfordern.

Abschnitt 3
Besonderer Datenschutz

§ 28
Datenverarbeitung für wissenschaftliche Zwecke

(1) Öffentliche Stellen dürfen personenbezogene Daten ohne Einwilligung für ein bestimmtes Forschungsvorhaben erheben, speichern, verändern, nutzen und an andere Stellen oder Personen zu diesem Zweck übermitteln, wenn

- a) schutzwürdige Belange des Betroffenen wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden,
- b) eine Rechtsvorschrift dies vorsieht oder
- c) das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann.

Der Empfänger darf die übermittelten Daten nicht für andere Zwecke verwenden.

(2) Die 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 bestimmbar Person zugeordnet werden können. Sie sind zu löschen, sobald der Forschungszweck dies erlaubt.

(3) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen diesem personenbezogene Daten nur übermittelt werden, wenn er sich verpflichtet, die Vorschriften des Absatzes 1 Satz 2 und des Absatzes 2 einzuhalten.

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

- a) der Betroffene eingewilligt hat oder
- b) dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 29
Datenverarbeitung bei Dienst- und
Arbeitsverhältnissen

(1) Personenbezogene Daten von Bewerbern und Beschäftigten dürfen nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher, planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder in einer Rechtsvorschrift, einem Tarifvertrag oder einer Dienst- oder Betriebsvereinbarung vorgesehen ist. Abweichend von § 16 Abs.1 ist eine Übermittlung der Daten von Beschäftigten an Personen und Stellen außerhalb des öffentlichen Bereiches nur zulässig, wenn der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder der Betroffene eingewilligt hat. Die Datenübermittlung an einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

(1a) Auf die Verarbeitung von Personalaktendaten der Arbeitnehmer und Auszubildenden finden die für Beamte geltenden Vorschriften des Landesbeamtengesetzes entsprechend Anwendung, es sei denn, besondere Rechtsvorschriften oder tarifliche Vereinbarungen gehen vor.

(2) Die Speicherung, Veränderung oder Nutzung der bei medizinischen oder psychologischen Untersuchungen und Tests zum Zwecke der Eingehung eines Dienst- oder Arbeitsverhältnisses erhobenen Daten ist nur mit schriftlicher Einwilligung des Bewerbers zulässig. Die Einstellungsbehörde darf vom untersuchenden Arzt in der Regel nur die Übermittlung des Ergebnisses der Eignungsuntersuchung und dabei festgestellter Risikofaktoren verlangen.

(3) Personenbezogene Daten, die vor der Eingehung eines Dienst- oder Arbeitsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt, es sei denn, dass der Betroffene in die weitere Speicherung eingewilligt hat. Nach Beendigung eines Dienst- oder Arbeitsverhältnisses sind personenbezogene Daten zu löschen, wenn diese Daten nicht mehr benötigt werden, es sei denn, dass Rechtsvorschriften entgegenstehen; § 19 Abs. 2 Satz 2 und 3 sowie § 19 Abs. 4 finden Anwendung.

(4) Soweit Daten der Beschäftigten im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach § 10 Abs. 2 gespeichert werden, dürfen sie nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

§ 30

Fernmessen und Fernwirken

(1) Öffentliche Stellen dürfen ferngesteuerte Messungen oder Beobachtungen (Fernmessdienste) in Wohnungen oder Geschäftsräumen nur vornehmen, wenn der Betroffene zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes unterrichtet worden ist und nach der Unterrichtung schriftlich eingewilligt hat. Entsprechendes gilt, soweit eine Übertragungseinrichtung dazu dienen soll, in Wohnungen oder Geschäftsräumen andere Wirkungen auszulösen (Fernwirkdienste). Die Einrichtung von Fernmess- und Fernwirkdiensten ist nur zulässig, wenn der Betroffene erkennen kann, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist; dies gilt nicht für Fernmess- und Fernwirkdienste der Versorgungsunternehmen. Der Betroffene kann seine Einwilligung jederzeit widerrufen, soweit dies mit der Zweckbestimmung des Dienstes vereinbar ist. Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, dass der Betroffene nach Absatz 1 Satz 1 oder 2 einwilligt. Verweigert oder widerruft er seine Einwilligung, so dürfen ihm keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

(3) Soweit im Rahmen von Fernmess- oder Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Sie sind zu löschen, sobald sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind.

§ 31

Verarbeitung personenbezogener Daten durch den Landtag

(1) Die Landesregierung darf personenbezogene Daten, die für andere Zwecke erhoben worden sind, zur Beantwor-

tung parlamentarischer Anfragen sowie zur Vorlage von Unterlagen und Berichten an den Landtag in dem dafür erforderlichen Umfang verwenden. Eine Übermittlung der Daten zu einem der in Satz 1 genannten Zwecke ist nicht zulässig, wenn dies wegen des streng persönlichen Charakters der Daten für den Betroffenen unzumutbar ist oder wenn der Eingriff in sein informationelles Selbstbestimmungsrecht unverhältnismäßig ist. Dies gilt nicht, wenn im Hinblick auf § 2 Abs. 1a Satz 2 oder durch sonstige geeignete Maßnahmen sichergestellt ist, dass schutzwürdige Interessen der Betroffenen nicht beeinträchtigt werden. Besondere gesetzliche Übermittlungsverbote bleiben unberührt.

(2) Von der Landesregierung übermittelte personenbezogene Daten dürfen nicht in Landtagsdrucksachen aufgenommen oder in sonstiger Weise allgemein zugänglich gemacht werden. Dies gilt nicht, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange der Betroffenen beeinträchtigt werden.

§ 32 (aufgehoben)

§ 33 Datenverarbeitung zu journalistisch-redaktionellen Zwecken

(1) Soweit öffentliche Stellen – insbesondere als Unternehmen oder Hilfsunternehmen der Presse, des Rundfunks oder des Films – personenbezogene Daten ausschließlich zu eigenen meinungsbildenden journalistisch-redaktionellen Zwecken verarbeiten, gilt von den Vorschriften dieses Gesetzes nur § 10.

(2) Führt die journalistisch-redaktionelle Verarbeitung personenbezogener Daten 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.

§ 33a Öffentliche Auszeichnungen und Ehrungen

(1) Zur Vorbereitung öffentlicher Auszeichnungen und Ehrungen dürfen die zuständigen Stellen die dazu erforderli-

chen Daten auch ohne Kenntnis des Betroffenen verarbeiten. Eine Verarbeitung dieser Daten für andere Zwecke ist nur mit Einwilligung des Betroffenen zulässig.

(2) Auf Anforderung der in Absatz 1 genannten Stellen dürfen andere öffentliche Stellen die zur Vorbereitung der Auszeichnung oder Ehrung erforderlichen Daten übermitteln.

(3) Die in Absatz 1 genannten Stellen haben den Betroffenen auf Antrag Auskunft zu erteilen über

- a) die zu seiner Person gespeicherten Daten,
- b) den Zweck und die Rechtsgrundlage der Speicherung sowie
- c) die Herkunft der Daten.

Die Form der Auskunftserteilung ist nach pflichtgemäßem Ermessen zu bestimmen. Im Übrigen findet § 18 keine Anwendung.

(4) Die Absätze 1 und 2 finden keine Anwendung, wenn der Daten verarbeitenden Stelle bekannt ist, dass der Betroffene seiner öffentlichen Auszeichnung oder Ehrung oder der mit ihr verbundenen Datenverarbeitung widersprochen hat.

§ 33b Begnadigungsverfahren

In Begnadigungsverfahren ist die Verarbeitung personenbezogener Daten zulässig, soweit sie zur Ausübung des Gnadenrechts durch die zuständigen Stellen erforderlich ist. Die Datenverarbeitung unterliegt nicht der Kontrolle durch den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht.

§ 33c Videobeobachtung und -aufzeichnung

(1) Öffentliche Stellen dürfen mit optisch-elektronischen Einrichtungen öffentlich zugängliche Räume überwachen, soweit dies

- 1. zur Erfüllung ihrer Aufgaben,

2. zur Wahrnehmung des Hausrechts,
3. zum Schutz des Eigentums oder Besitzes oder
4. zur Kontrolle von Zugangsberechtigungen

erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen.

(2) Der Umstand der Videoüberwachung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen. Für einen anderen Zweck dürfen sie nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist. § 19 Abs. 2 Satz 1 Buchstabe b bleibt unberührt.

(4) Werden durch Videoaufnahmen gewonnene personenbezogene Daten verändert, übermittelt oder sonst genutzt, ist der Betroffene zu benachrichtigen. § 12 Abs. 5 gilt entsprechend.

§ 33d Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt, muss den Betroffenen

1. über ihre Identität und Anschrift,
2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,
3. darüber, wie er seine Rechte nach den §§ 18 und 19 ausüben kann, und

4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen

unterrichten, soweit er nicht bereits Kenntnis erlangt hat.

(2) Kommunikationsvorgänge, die eine Verarbeitung auslösen, müssen für den Betroffenen erkennbar sein.

§ 34

(außer Kraft getreten)

§ 35

(außer Kraft getreten)

§ 36

(außer Kraft getreten)

§ 37

(außer Kraft getreten)

Abschnitt 4

**Straf- und Bußgeldvorschriften;
Übergangsvorschriften**

§ 38

Ordnungswidrigkeiten, Strafvorschrift

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften dieses Gesetzes oder einer anderen Rechtsvorschrift über den Datenschutz personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, unbefugt verwendet, verändert, übermittelt, weitergibt, zum Abruf bereit hält, den Personenbezug herstellt oder löscht oder
2. abrufen, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung oder Weitergabe an sich oder andere veranlasst.

Ordnungswidrig handelt auch, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbar-

ren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50 000 Euro geahndet werden.

(3) Wer gegen Entgelt oder in der Absicht sich oder einen anderen zu bereichern oder einen anderen zu schädigen, eine der in Absatz 1 genannten Handlungen begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle und der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht.

**§ 39
(aufgehoben)**

**§ 40
Übergangsvorschriften**

(1) In Akten, die bei Inkrafttreten des Gesetzes vorhanden waren, ist die Berichtigung, Löschung oder Sperrung vorzunehmen, wenn die Daten verarbeitende Stelle deren Voraussetzungen bei der Erfüllung ihrer laufenden Aufgaben oder aufgrund eines Überprüfungsersuchens des Betroffenen feststellt.

(2) Die §§ 34, 35, 36 und 37 treten mit Ablauf des 31. Dezember 2009 außer Kraft.

**§ 40a
Einschränkung von Grundrechten**

Durch dieses Gesetz wird das Grundrecht auf Datenschutz (Artikel 11 Abs. 1 der Verfassung des Landes Brandenburg) eingeschränkt.

§ 41
(Inkrafttreten)

Anlage 1
(aufgehoben)

Anlage 2
(aufgehoben)