

# Gesetz zum Schutz personenbezogener Daten im Land Brandenburg

## (Brandenburgisches Datenschutzgesetz - BbgDSG)

in der Fassung der Bekanntmachung  
vom 9. März 1999 (GVBl. I S. 66)

zuletzt geändert durch das Gesetz zur Änderung von verwaltungsverfahren-, ordnungs-,  
datenschutz-, statistik- und vermessungs- und liegenschaftsrechtlichen Bestimmungen  
aus Anlass der Euro-Einführung vom 18. Dezember 2001 (GVBl. I S. 298)

---

### 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](#) Verfahrens- und Anlagenverzeichnis
- [§ 9](#) Automatisiertes Abrufverfahren und regelmäßige Datenübermittlung
- [§ 10](#) Technische und organisatorische Maßnahmen
- [§ 11](#) Verarbeitung personenbezogener Daten im Auftrag
- [§ 11a](#) Wartung
- [§ 11b](#) Grundsätze der System- und Verfahrensgestaltung
- [§ 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](#) Ausnahmsweise Übermittlung an Stellen außerhalb der Europäischen Union

##### Unterabschnitt 3

##### Rechte des Betroffenen

- [§ 18](#) Auskunft und Benachrichtigung sowie 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

### **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

[§ 34](#) Personenbezogene Daten aus ehemaligen Einrichtungen

[§ 35](#) Verarbeitung personenbezogener Daten aus ehemaligen Einrichtungen

[§ 36](#) Widerspruchsrecht

[§ 37](#) Sperrung personenbezogener Daten aus ehemaligen Einrichtungen

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

[§ 38](#) Straftaten

[§ 39](#) Ordnungswidrigkeiten

[§ 40](#) Übergangsvorschriften

[§ 40a](#) Einschränkung von Grundrechten

[§ 41](#) Inkrafttreten

[Anlage 1](#) - Anforderungskatalog zu § 11a Abs. 1 Satz 3

[Anlage 2](#) - Mindestvertragsinhalt zu § 11a Abs. 2 Satz 2

---

## **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 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 nichtöffentliche 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 nur die Vorschriften des Abschnitts 2 sowie die §§ [7a](#), [8](#) und [28 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. der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts, die am Wettbewerb teilnehmen,

personenbezogene Daten zu wirtschaftlichen Zwecken oder Zielen verarbeiten. Im übrigen sind mit Ausnahme der §§ [32](#) sowie [36 bis 38](#) die für nicht-öffentliche Stellen geltenden Vorschriften des [Bundesdatenschutzgesetzes](#) einschließlich der Straf- und Bußgeldvorschriften anzuwenden. Unbeschadet der Regelung des Absatzes 1 Satz 1 gelten Schulen der Gemeinden und Gemeindeverbände, soweit sie in inneren Schulangelegenheiten personenbezogene Daten verarbeiten, als öffentliche Stellen im Sinne dieses Gesetzes.

(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 bestimmbaren 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 Bekannt geben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die datenverarbeitende Stelle weitergegeben oder zur Einsichtnahme bereitgehalten werden oder dass der Dritte zum Abruf in einem automatisierten Verfahren bereitgehaltene Daten 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 angewendeten 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 bestimmbaren natürlichen Person zugeordnet werden können und

2. Pseudonymisieren das Verändern personenbezogener Daten mittels der Vergabe von Pseudonymen derart, dass die Einzelangaben über persönliche und sachliche Verhältnisse von Unbefugten nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(4) Im Sinne dieses Gesetzes ist

1. datenverarbeitende 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 außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene sowie diejenige Person oder Stelle, die im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union Daten im Auftrag verarbeitet.

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

(6) Soweit bereichsspezifische Gesetze den Dateibegriff verwenden, ist eine Datei eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet 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) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

- a) dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
- b) der Betroffene ohne jeden Zweifel eingewilligt hat.

(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) 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. 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 datenverarbeitenden 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**

Die Verarbeitung personenbezogener Daten über

- a) die rassische und ethnische Herkunft,
- b) politische Meinungen,
- c) religiöse oder weltanschauliche Überzeugungen,
- d) die Gewerkschaftszugehörigkeit,
- e) die Gesundheit oder
- f) das Sexualleben

ist nur zulässig, wenn sie in einer bereichsspezifischen Rechtsvorschrift geregelt ist, die den Zweck der Verarbeitung bestimmt sowie angemessene Garantien zum Schutze des Rechtes auf informationelle Selbstbestimmung vorsieht. Abweichend von Satz 1 ist die Verarbeitung dieser Daten zulässig,

- a) wenn der Betroffene ausdrücklich eingewilligt hat,
- b) auf der Grundlage der §§ [15](#), [28](#) und [29](#) oder
- c) wenn sie ausschließlich im Interesse des Betroffenen liegt und der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht vorab gehört worden ist.

#### **§ 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 und Benachrichtigung über die zu seiner Person gespeicherten Daten sowie Einsicht in Akten ([§ 18](#)),

2. Gegenvorstellung auf Grund eines schutzwürdigen besonderen persönlichen Interesses (§ [4b](#)),
3. Einsicht in das Verzeichnisse (§ [8 Abs. 5](#)),
4. Berichtigung, Löschung oder Sperrung der zu seiner Person gespeicherten Daten (§ [19](#)),
5. Schadensersatz (§ [20](#)) und
6. Anrufung des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (§ [21 Abs. 1](#)).

Diese Rechte können auch durch die Einwilligung des Betroffenen nicht ausgeschlossen oder beschränkt werden. Sie sind gegenüber der jeweiligen datenverarbeitenden Stelle geltend zu machen.

(2) Werden die Daten des Betroffenen in einem automatisierten Verfahren gespeichert, bei dem mehrere Stellen speicherungs berechtigt sind, und ist der Betroffene nicht in der Lage, die datenverarbeitende Stelle festzustellen, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die datenverarbeitende Stelle weiterzuleiten. Der Betroffene ist über die Weiterleitung und die datenverarbeitende 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 datenverarbeitende Stelle unterrichten. In diesem Fall richtet sich das weitere Vorgehen nach § [18 Abs. 8](#).

(3) Gibt eine öffentliche Stelle für das Erfassen einer Leistung, das Erkennen einer Person oder für einen anderen Zweck einen Datenträger heraus, auf dem oder durch den personenbezogene Daten des jeweiligen Inhabers dieses Datenträgers automatisiert nach Maßgabe des § [4 Abs. 1](#) als Chipkarte oder in anderer Form verarbeitet werden, hat sie sicherzustellen, dass er dies erkennen und seine ihm nach Absatz 1 zustehenden Rechte ohne unverhältnismäßigen Aufwand geltend machen kann. Der Inhaber ist bei Ausgabe 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. Die Ausgabe und Verwendung von Datenträgern nach Satz 1 darf für die Betroffenen nicht mit Vergünstigungen verbunden sein, die über das durch die Technik bedingte Maß hinausgehen.

## **§ 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 Rechtsvorschriften über den Datenschutz sicherzustellen. Sie haben insbesondere dafür zu sorgen, dass die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, gewährleistet 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.

(3) Der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf hinsichtlich der im Verzeichnisse festzulegenden Angaben (§ [8](#)

[Abs. 2](#)) der schriftlichen Freigabe; dabei ist auch zu untersuchen, ob von diesen Verfahren spezifische Risiken für die Rechte und Freiheiten der Betroffenen ausgehen können. Die Freigabe darf nur erklärt werden, wenn sichergestellt ist, dass diese Risiken nicht bestehen oder durch technische und organisatorische Maßnahmen beherrscht werden können. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten zuzuleiten. In der Landesverwaltung ist die Freigabe durch diejenige oberste Landesbehörde zu erklären, die für die dem automatisierten Verfahren zugrunde liegende Rechtsmaterie zuständig ist. Im übrigen erfolgt die Freigabe durch die datenverarbeitende Stelle. Entsprechendes gilt für wesentliche Änderungen des Verfahrens.

### **§ 7a Behördlicher Datenschutzbeauftragter**

(1) Datenverarbeitende 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.

(2) Der behördliche Datenschutzbeauftragte kann sich in dieser Funktion unmittelbar an die Leitung der datenverarbeitenden Stelle wenden. Er ist in seiner Eigenschaft als behördlicher Datenschutzbeauftragter weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.

(3) Die datenverarbeitenden Stellen können einen Bediensteten einer anderen datenverarbeitenden Stelle zum behördlichen Datenschutzbeauftragten bestellen.

(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) Die behördlichen Datenschutzbeauftragten haben die Aufgabe, die datenverarbeitenden Stellen bei der Ausführung der Datenschutzvorschriften zu unterstützen. Zu ihren Aufgaben gehört es insbesondere

1. auf die Beachtung der Datenschutzvorschriften und deren Einhaltung hinzuwirken,
2. die bei der Verarbeitung tätigen Personen mit den Bestimmungen dieses Gesetzes und anderer für die datenverarbeitende Stelle einschlägigen Rechtsvorschriften vertraut zu machen und
3. die datenverarbeitende Stelle bei der Umsetzung der nach [§ 7 Abs. 3](#) und nach den [§§ 8, 10, 11, 11a](#) und [26](#) erforderlichen Maßnahmen zu unterstützen.

Soweit keine gesetzliche Regelung entgegensteht, kann er die zur Erfüllung seiner Aufgaben notwendige Einsicht in personenbezogene Datenverarbeitungsvorgänge nehmen.

### **§ 8 Verfahrens- und Anlagenverzeichnis**

(1) Jede datenverarbeitende Stelle, die personenbezogene Daten verarbeitet, führt ein Verzeichnis der automatisierten Verfahren (Verfahrensverzeichnis) und ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen (Anlagenverzeichnis); die Verzeichnisse enthalten auch die Angaben über die Verfahren und Anlagen, die für die Stelle in Fällen von Datenverarbeitung im Auftrag eingesetzt werden.

(2) Das Verfahrensverzeichnis hat folgende Angaben zu enthalten:

1. Bezeichnung des Verfahrens,
2. Name und Anschrift des für die Verarbeitung Verantwortlichen,
3. Zweckbestimmung und Rechtsgrundlagen der Verarbeitung,

4. Art der gespeicherten Daten,
5. Kreis der Betroffenen,
6. Art der regelmäßig an Dritte zu übermittelnden oder regelmäßig innerhalb der datenverarbeitenden Stelle weiterzugebenden Daten und deren Empfänger,
7. Art sowie Herkunft der regelmäßig von Dritten empfangenen Daten,
8. Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung,
9. Datenübermittlungen in Drittländer sowie deren Namen,
10. allgemeine Beschreibung der Art der eingesetzten Datenverarbeitungsanlagen und der technischen und organisatorischen Maßnahmen nach [§ 10](#) und
11. welche Teile des Verfahrens der Datenverarbeitung räumlich außerhalb der datenverarbeitenden Stelle durchgeführt werden.

(3) Die Führung des Verfahrensverzeichnisses soll dem behördlichen Datenschutzbeauftragten übertragen werden. Die datenverarbeitende Stelle hat dem behördlichen Datenschutzbeauftragten die in Absatz 2 aufgeführten Angaben rechtzeitig vor Einführung oder wesentlicher Änderung des Verfahrens mitzuteilen, um ihm die Prüfung des Verfahrens zu ermöglichen.

(4) Die Führung eines eigenen Anlagenverzeichnisses kann entfallen, wenn ein Geräteverzeichnis nach haushaltsrechtlichen Vorschriften geführt wird, sofern die Geräte in dem gleichen Umfang technisch beschrieben werden, wie es zum Zweck der Datenschutzkontrolle geboten ist; zu diesen Angaben gehören auch die Bezeichnungen gegenwärtig verwendeter Betriebssysteme.

(5) Das Anlagen- und das Verfahrensverzeichnis sind bei wesentlichen Änderungen zu aktualisieren.

(6) Die Angaben des Verfahrensverzeichnisses gemäß Absatz 2 Nr. 1 bis 7 und 9 können bei der datenverarbeitenden Stelle von jedem eingesehen werden; dies gilt auch für die Angaben gemäß Absatz 2 Nr. 10, soweit dadurch die Sicherheit des Verfahrens nicht beeinträchtigt wird. 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 datenverarbeitende Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt.

(7) Absatz 2 gilt nicht für Verfahren,

- a) 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 offensteht,
- b) soweit mit ihnen Datensammlungen erstellt werden, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden, oder
- c) die unter Einsatz handelsüblicher Schreibprogramme ablaufen.

(8) Die Landesregierung wird ermächtigt, durch [Rechtsverordnung](#) das Nähere zur Ausgestaltung des Anlagen- und Verfahrensverzeichnisses zu regeln, insbesondere zum Zweck der Vereinfachung des Verfahrens und zur Entlastung der datenverarbeitenden Stellen.

## § 9

### Automatisiertes Abrufverfahren und regelmäßige Datenübermittlung

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist nur zulässig, soweit dies durch Bundes- oder Landesrecht bestimmt ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufes bleiben unberührt.

(2) Die Minister werden ermächtigt, für die Behörden und Einrichtungen ihres Geschäftsbereiches sowie für die der Rechtsaufsicht des Landes unterliegenden sonstigen öffentlichen Stellen die Einrichtung automatisierter Abrufverfahren durch Rechtsverordnung zuzulassen. Ein solches Verfahren darf nur eingerichtet werden, soweit dies unter Berücksichtigung des informationellen Selbstbestimmungsrechts des betroffenen Personenkreises und der Aufgaben der beteiligten Stellen angemessen ist. Die Datenempfänger, die Datenart und der Zweck des Abrufes sind festzulegen. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht ist zu unterrichten.

(3) Die am Abrufverfahren beteiligten Stellen haben die nach [§ 10](#) erforderlichen Maßnahmen zu treffen.

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

(5) Personenbezogene Daten dürfen für Stellen außerhalb des öffentlichen Bereiches nicht zum automatisierten Abruf bereitgehalten werden; dies gilt nicht für den Betroffenen.

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

(7) Absatz 1 Satz 1 und Absatz 2 Satz 1 und 4 sowie Absatz 5 finden keine Anwendung, soweit die zur Übermittlung vorgesehenen Daten mit schriftlicher Einwilligung der Betroffenen zum Zwecke der Übermittlung im automatisierten Abrufverfahren gespeichert sind, [§ 4 Absatz 2](#) Satz 2 und 3 gilt entsprechend.

(8) Die Absätze 1 bis 7 sind auf die Zulassung regelmäßiger Datenübermittlungen entsprechend anzuwenden.

## **§ 10**

### **Technische und organisatorische Maßnahmen**

(1) Die datenverarbeitenden 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 je nach Art der zu schützenden personenbezogenen Daten geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten benutzt werden können (Benutzerkontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können (Zugriffskontrolle),
4. zu verhindern, dass personenbezogene Daten unbefugt oder zufällig gespeichert, zur Kenntnis genommen, verändert, kopiert, übermittelt, entfernt, vernichtet oder sonst verarbeitet werden (Datenverarbeitungskontrolle),
5. festzustellen, wer welche personenbezogenen Daten zu welcher Zeit verarbeitet hat und wohin sie übermittelt werden sollen oder übermittelt worden sind (Verantwortlichkeitskontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. eine Überprüfung aller wesentlichen Verarbeitungsschritte der Datenverarbeitungsanlage und des -verfahrens durch eine Dokumentation zu ermöglichen (Dokumentationskontrolle) und
8. die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

(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.

(4) Soweit Vorentwürfe und Notizen nicht Bestandteil eines Vorganges werden und personenbezogene Daten enthalten, ist eine ordnungsgemäße Vernichtung zu gewährleisten.

## **§ 11**

### **Verarbeitung personenbezogener Daten im Auftrag**

(1) Werden personenbezogene Daten im Auftrag einer datenverarbeitenden 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. Die in [§ 5](#) Abs. 1 genannten Rechte sind ihr gegenüber geltend zu machen. Sofern die Bestimmungen dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich, sofern die Datenverarbeitung im Geltungsbereich dieses Gesetzes vorgenommen wird, der Kontrolle des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht unterwirft. Erfolgt die Durchführung des Auftrages außerhalb des Geltungsbereiches dieses Gesetzes durch eine nicht-öffentliche Stelle, so ist sicherzustellen, dass sich diese Stelle der Kontrolle des Landesbeauftragten für den Datenschutz, in dessen Land die Verarbeitung erfolgt, unterwirft, soweit dieser hierzu durch Landesrecht befugt ist. Bei einer Auftragsdurchführung außerhalb des Geltungsbereiches dieses Gesetzes ist die für den Ort der Auftragsdurchführung zuständige Datenschutzkontrollbehörde zu unterrichten. Der Auftraggeber hat den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht und die im Land Brandenburg nach [§ 38](#) des Bundesdatenschutzgesetzes zuständige Aufsichtsbehörde über die Beauftragung zu unterrichten. Soweit der Auftragnehmer eine nicht-öffentliche Stelle ist, bedarf die Auftragserteilung der Zustimmung; bei öffentlichen Stellen des Landes erteilt die zuständige oberste Landesbehörde, bei Gemeinden und Gemeindeverbänden der Minister des Innern. Die Zustimmung ist vor Abschluß des Vertrages einzuholen.

(2) Der Auftragnehmer ist unter Berücksichtigung der Eignung der von ihr getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist unter Festlegung des Gegenstandes und des Umfangs der Datenverarbeitung, der technischen und organisatorischen Maßnahmen und etwaiger Unterauftragsverhältnisse schriftlich zu erteilen. Für ergänzende Weisungen gilt Satz 2 entsprechend. 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. Weisungen, die sich auf eine Datenverarbeitung richten, die gegen dieses Gesetz oder andere Rechtsvorschriften über den Datenschutz verstoßen, sind nicht durchzuführen. Dasselbe gilt, wenn Daten verarbeitet werden sollen, die nach Ansicht des Auftragnehmers unter Verstoß gegen Rechtsvorschriften erlangt worden sind.

(4) Ist der Auftragnehmer eine in [§ 2](#) Abs. 1 Satz 1 oder 2 genannte Stelle des Landes, gelten für ihn neben Absatz 3 nur die [§§ 6](#) und [10](#) sowie [21](#), [23](#), [25](#), [26](#), [38](#) und [39](#).

(5) Bezieht sich der Auftrag auf die Verarbeitung von Daten, für die gesetzliche Geheimhaltungspflichten bestehen oder die Berufs- oder besonderen Amtsgeheimnissen unterfallen, die nicht auf gesetzlichen Vorschriften beruhen, sind besondere Maßnahmen nach Absatz 2 Satz 2 zu treffen, die eine Wahrung der Geheimnisse sicherstellen. Darüber hinaus sollen an nicht-öffentliche

Stellen Aufträge nach Satz 1 nur vergeben werden, wenn überwiegende schutzwürdige Interessen der Betroffenen nicht entgegenstehen. Satz 2 gilt nicht, wenn sich der Auftrag nur auf

- a) das Erfassen, Aufnehmen, Aufbewahren oder Vernichten von Daten,
- b) das Übertragen von Daten von einem auf ein anderes Speichermedium oder
- c) die Verarbeitung von Daten, die aus der Sicht der auftragnehmenden Person oder Stelle nicht oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,

bezieht, und sofern technische und organisatorische Maßnahmen ergriffen worden sind, durch die sichergestellt wird, dass der Auftragnehmer nur soweit es für die Aufgabenerfüllung unerlässlich ist, die Daten zur Kenntnis nehmen kann.

(6) Sofern Unterauftragsverhältnisse vorgesehen sind oder zugelassen werden sollen, ist vertraglich sicherzustellen, dass die datenschutzrechtlichen Pflichten in dem gleichen Umfang eingehalten werden, wie sie im Auftragsverhältnis mit der öffentlichen Stelle festgelegt sind; Absatz 1 Satz 3 bis 6 gilt 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 datenverarbeitende Stelle durch technische und organisatorische Maßnahmen sicherzustellen, dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann. Dabei sind insbesondere die in der [Anlage 1](#) genannten Anforderungen zu erfüllen. [§ 10](#) Abs. 1 Satz 2 gilt entsprechend.

(2) Eine Wartung durch andere Stellen darf über die Anforderungen nach Absatz 1 hinaus nur aufgrund schriftlicher Vereinbarungen erfolgen. Darin sind die im Rahmen der Wartung notwendigen technischen und organisatorischen Maßnahmen gemäß [Anlage 2](#) festzulegen. Die mit Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

(3) Ist im Rahmen einer Prüfung nach [§ 11b](#) festgestellt worden, dass bei Wartungsarbeiten nur ein Zugriff auf Daten in verschlüsselter, pseudonymisierter oder anonymisierter Form gegeben ist, so dass seitens der mit der Wartung betrauten Stelle eine Reidentifizierung von Betroffenen nicht möglich ist, sind nur Maßnahmen nach Absatz 2 Satz 1 und 3 erforderlich. Ein Zugriff darf nur zweckgebunden erfolgen.

(4) Im Sinne dieses Gesetzes ist

- a) 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,
- b) 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 und
- c) Verschlüsselung das Ersetzen von Klartextbegriffen oder Zeichen durch andere in der Weise, dass der Klartext nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wieder lesbar gemacht werden kann.

### **§ 11b Grundsätze der System- und Verfahrensgestaltung**

(1) Die datenverarbeitenden Stellen können die Inanspruchnahme von Leistungen auch anonym oder unter Pseudonym ermöglichen, soweit dies technisch durchführbar ist. Die Person, die das Angebot in Anspruch nehmen will, ist über diese Möglichkeit zu informieren.

(2) Bei der Gestaltung und Auswahl informationstechnischer Produkte und Verfahren hat die datenverarbeitende Stelle sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu verarbeiten. Sie hat zu prüfen, ob deren Einsatz mit den Regelungen des Datenschutzrechts vereinbar ist. Produkte und Verfahren, deren Vereinbarkeit mit den Regeln des Datenschutzrechts in einem förmlichen Verfahren geprüft und positiv bewertet worden sind, sollen vorrangig berücksichtigt werden.

### **§ 11c Datenschutzaudit**

Die öffentlichen Stellen können zur Verbesserung von Datenschutz und Datensicherheit sowie zum Erreichen größtmöglicher 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. Dazu sollen durch das zuständige Ministerium im Einvernehmen mit dem Ministerium des Innern und dem Ministerium der Justiz Verwaltungsvorschriften erlassen werden. Diese sind im Amtsblatt für das Land Brandenburg zu veröffentlichen.

(2) Personenbezogene Daten sind grundsätzlich beim Betroffenen mit seiner Kenntnis zu erheben. Ohne seine Kenntnis dürfen sie bei anderen Stellen oder Personen unter der Voraussetzung des [§ 13 Abs. 2](#) Satz 1 Buchstaben 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. Durch die Art und Weise des Erhebens dürfen schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden.

(3) Werden Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist er über den Verwendungszweck aufzuklären. Die Aufklärungspflicht umfaßt bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Werden die Daten auf Grund einer Rechtsvorschrift erhoben, so ist der Betroffene in geeigneter Weise über diese aufzuklären. Soweit eine Auskunftspflicht besteht oder die Angaben Voraussetzung für die Gewährung von Rechten sind, ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen.

(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 beim Betroffenen ohne seine Kenntnis erhoben, so ist er davon zu benachrichtigen, sobald die rechtmäßige Erfüllung der Aufgabe dadurch nicht mehr gefährdet wird. Absatz 3 Satz 1 und 2 gelten entsprechend.

### **§ 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 weiterverarbeitet werden, für die sie erhoben worden sind. Daten, von denen die Stelle ohne

Erhebung Kenntnis erlangt hat, dürfen nur für Zwecke genutzt werden, für die sie erstmals gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken weiterverarbeitet 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 datenverarbeitende 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.

Im Falle des Satzes 1 Buchstabe b darf die Erbringung einer Leistung nicht von der Einwilligung der betroffenen Person in eine Verarbeitung ihrer Daten für andere Zwecke abhängig gemacht werden. Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der datenverarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, findet Satz 1 Buchstaben 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 auf Grund 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 Religionsgesellschaften**

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 Buchstaben 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 im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union richtet sich nach [§ 4](#).

(2) Für die Übermittlung personenbezogener Daten an Stellen außerhalb des Geltungsbereichs der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union 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 Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

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

### **§ 17a**

#### **Ausnahmsweise Übermittlung an Stellen außerhalb der Europäischen Union**

(1) Sofern Stellen nach [§ 17 Abs. 2](#) kein angemessenes Datenschutzniveau gewährleisten, ist eine Übermittlung personenbezogener Daten nach [§ 17](#) Abs. 1 nur zulässig, sofern

- a) der Betroffene seine Einwilligung gegeben hat,
- b) die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
- c) die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
- d) die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu Zwecken verarbeitet werden dürfen, die mit den Zwecken zu vereinbaren sind, zu deren Erfüllung sie ihr übermittelt werden.

(2) Unbeschadet des Absatzes 1 kann die datenverarbeitende Stelle eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten zulassen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist. Die datenverarbeitenden Stellen teilen dem Ministerium des Innern die Fälle mit, in denen Stellen nach [§ 17 Abs. 2](#) kein angemessenes Datenschutzniveau aufweisen und sie eine Genehmigung nach Satz 1 erteilt haben.

### **Unterabschnitt 3 Rechte des Betroffenen**

#### **§ 18**

#### **Auskunft und Benachrichtigung sowie Einsicht in Akten**

(1) Dem Betroffenen ist von der datenverarbeitenden Stelle auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung,
3. den logischen Aufbau der automatisierten Verarbeitung der zu seiner Person gespeicherten Daten sowie
4. die Herkunft der Daten, den Zweck der Übermittlung und die Empfänger von regelmäßigen Übermittlungen und die Teilnehmer eines automatisierten Abrufverfahrens, auch soweit diese Angaben nicht zu seiner Person gespeichert sind, aber mit vertretbarem Aufwand festgestellt werden können. Sind die Daten in einem automatisierten Verfahren gespeichert, so umfasst die Auskunft auch die Empfänger von Übermittlungen innerhalb der letzten zwei Jahre. In Akten und bei nicht-automatisierter Speicherung sind Übermittlungen zu dokumentieren.

(2) Werden personenbezogene Daten automatisiert gespeichert, so ist der Betroffene von dieser Tatsache schriftlich zu benachrichtigen. Die Benachrichtigung kann zusammen mit der Erhebung erfolgen.

(2a) Eine Pflicht zur Benachrichtigung nach Absatz 2 besteht nicht, wenn

- a) die Daten beim Betroffenen mit dessen Kenntnis erhoben worden sind,
- b) die Verarbeitung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist,
- c) der Betroffene auf andere Weise Kenntnis von der Verarbeitung seiner Daten erlangt oder
- d) die Benachrichtigung des Betroffenen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert.

(3) Die Absätze 1 und 2 gelten nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

(4) Die datenverarbeitende 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.

(5) Die Verpflichtung zur Auskunftserteilung oder zur Gewährung der Akteneinsicht sowie zur Benachrichtigung entfällt, soweit die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen eines Dritten geheimgehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muß.

(6) 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.

(7) 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.

(8) 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 datenverarbeitenden 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 datenverarbeitende 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 über die Speicherung hinaus nicht mehr weiterverarbeitet werden, es sei denn, dass dies zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der datenverarbeitenden Stelle oder eines Dritten liegenden Gründen unerlässlich ist oder der Betroffene eingewilligt hat.

(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.

## **§ 20 Schadensersatz**

(1) Wird dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung seiner personenbezogenen Daten ein Schaden zugefügt, so ist ihm der Träger der datenverarbeitenden Stelle unabhängig von einem Verschulden zum Schadensersatz verpflichtet. In schweren Fällen kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen. Der Ersatzpflichtige haftet jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von 250 000 Euro.

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

(3) Weitergehende sonstige Schadensersatzansprüche 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 Brandenburg 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 ist verpflichtet, das Amt bis zur Bestellung eines Nachfolgers weiterzuführen; die Amtszeit gilt als entsprechend verlängert. 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 Sinne 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, anderer Vorschriften über den Datenschutz sowie die Einhaltung des Akteneinsichts- und Informationszugangsgesetzes gemäß [§ 11 Abs. 2](#) des Akteneinsichts- und Informationszugangsgesetzes bei öffentlichen Stellen, soweit sie nach diesem Gesetz seiner Kontrolle unterliegen oder sich gemäß [§ 11 Abs. 1 Satz 3](#) oder [§ 28 Abs. 4](#) seiner Kontrolle unterworfen haben.

(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. Er hat auf einzelgesetzliche Regelungen hinzuwirken. Er ist über Planungen des Landes zum Aufbau automatisierter Informationssysteme rechtzeitig zu unterrichten, sofern in den Systemen personenbezogene Daten verarbeitet werden sollen.

(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 weiterverarbeitet 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) Für die öffentlichen Stellen des Landes gilt [§ 24 Abs. 2 Satz 5](#) des Bundesdatenschutzgesetzes entsprechend.

## **§ 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, oder 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 Nrn. 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 auf Grund der Beanstandung des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht getroffen worden sind. Die in Absatz 1 Nrn. 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 Abs. 7](#) 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.

## **§ 27 Tätigkeitsberichte**

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht legt dem Landtag und der Landesregierung jährlich einen Bericht über seine Tätigkeit vor. Die Landesregierung legt hierzu regelmäßig innerhalb von vier Monaten nach Vorlage des Tätigkeitsberichtes ihre Stellungnahme dem Landtag vor; gleichzeitig gibt sie einen Bericht über die Tätigkeit der für den Datenschutz im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörde.

## **Abschnitt 3 Besonderer Datenschutz**

### **§ 28 Datenverarbeitung für wissenschaftliche Zwecke**

(1) Öffentliche Stellen dürfen personenbezogene Daten zu wissenschaftlichen Zwecken verarbeiten, soweit der Betroffene eingewilligt hat.

(2) 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) die zuständige oberste Aufsichtsbehörde festgestellt hat, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen überwiegt und der Zweck der Forschung nicht auf andere Weise oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Der Empfänger darf die übermittelten Daten nicht für andere Zwecke verwenden. Personen, die innerhalb einer öffentlichen Stelle auf Grund ihrer Zuständigkeiten Zugriff auf den jeweiligen Datenbestand haben, dürfen personenbezogene Daten ohne Einwilligung speichern, verändern und nutzen, wenn die übrigen Voraussetzungen des Satzes 1 vorliegen. In den Fällen des Satzes 1 haben die öffentlichen Stellen den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht zu unterrichten.

(3) 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 bestimmbarer Person zugeordnet werden können. Sie sind zu löschen, sobald der Forschungszweck dies erlaubt.

(4) 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 2 Satz 2 und des Absatzes 3 einzuhalten, und sich, sofern das Forschungsvorhaben im Geltungsbereich dieses Gesetzes durchgeführt werden soll, der Kontrolle des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht unterwirft. Bei einer Datenübermittlung an Stellen außerhalb des Geltungsbereiches dieses Gesetzes hat die übermittelnde Stelle die für den Empfänger zuständige Datenschutzkontrollbehörde zu unterrichten.

(5) 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) Daten von Bewerbern und Beschäftigten dürfen nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienstvereinbarung dies vorsieht. 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.

(2) Die Weiterverarbeitung 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) Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests des Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz des Beschäftigten dient.

(5) 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.

(6) Beurteilungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen 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 Beantwortung 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 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 erforderlichen Daten auch ohne Kenntnis des Betroffenen erheben und weiter 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 datenverarbeitenden 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**

#### **Videoüberwachung und -aufzeichnung**

(1) Öffentliche Stellen dürfen mit optisch-elektronischen Einrichtungen öffentlich zugängliche Räume beobachten (Videoüberwachung), soweit dies zu Erfüllung ihrer Aufgaben oder zur Wahrnehmung des Hausrechts erforderlich ist und überwiegende schutzwürdige Interessen Betroffener nicht beeinträchtigt werden. Das Bildmaterial darf gespeichert werden (Videoaufzeichnung), wenn die Tatsache der Aufzeichnung den Betroffenen durch geeignete Maßnahmen erkennbar gemacht ist. [§ 19 Abs. 2](#) Buchstabe b bleibt unberührt.

(2) Werden durch Videoaufnahmen gewonnene personenbezogene Daten verändert, übermittelt oder sonst genutzt, ist der Betroffene mit Angabe der Rechtsgrundlage zu benachrichtigen. [§ 12 Abs. 5](#) gilt entsprechend.

(3) Besondere Vorschriften bleiben unberührt.

### **§ 34**

#### **Personenbezogene Daten aus ehemaligen Einrichtungen**

(1) Waren personenbezogene Daten aus ehemaligen Einrichtungen vor dem 3. Oktober 1990 nach ihrer Zweckbestimmung überwiegend für Verwaltungsaufgaben gespeichert, die nach dem Grundgesetz von Behörden, Einrichtungen und sonstigen öffentlichen Stellen des Landes, den Gemeinden, Gemeindeverbänden oder sonstigen öffentlichen Stellen im Sinne des [§ 2](#) Abs. 1 Satz 1 wahrzunehmen sind, so stehen sie demjenigen Träger öffentlicher Verwaltung zu, der für die Verwaltungsaufgabe zuständig ist.

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

(3) Öffentliche und nicht-öffentliche Stellen sowie Personen, die personenbezogene Daten im Sinne des Absatzes 1 im Besitz haben, soweit diese nicht in den Verwaltungsvollzug übernommen worden sind, haben bis zum 1. Juli 1992 entsprechend [§ 8](#) Abs. 1 ein Verzeichnis zu erstellen und dieses dem Ministerium des Innern vorzulegen; entsprechendes gilt für vorhandene Aktenbestände und nicht-automatisiert verarbeitete Daten. Auf Verlangen des Ministeriums des Innern haben sie diese Dateien oder Akten sowie die zu ihrer Ordnung, Auffindung oder Auswertung dienenden Materialien und Träger sowie sämtliches Zubehör dem Ministerium des Innern oder einer von diesem benannten Behörde im Original und mit sämtlichen Ausfertigungen zur Einsicht vorzulegen und zu übergeben. Kopien dürfen von ihnen weder angefertigt noch behalten werden. Das Ministerium des Innern übergibt die Unterlagen den nach Absatz 1 zuständigen Behörden.

### **§ 35**

#### **Verarbeitung personenbezogener Daten aus ehemaligen Einrichtungen**

(1) Abweichend von [§ 13](#) Abs. 1 ist das Speichern, Verändern oder Nutzen personenbezogener Daten aus ehemaligen Einrichtungen durch die in [§ 34](#) Abs. 1 genannten 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 nicht nach [§ 36](#) widersprochen hat und
4. die Zuständigkeit und Verantwortlichkeit der datenverarbeitenden Stellen eindeutig bestimmt ist.

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

## **§ 36 Widerspruchsrecht**

(1) Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten widersprechen, wenn die Daten durch eine ehemalige Einrichtung erhoben und durch diese oder eine andere ehemalige Einrichtung gespeichert wurden und die Daten nach geltendem Recht nicht ohne seine Mitwirkung erhoben werden dürfen.

(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,
4. die nunmehr zuständige datenverarbeitende Stelle und
5. die bestehende Widerspruchsmöglichkeit

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

## **§ 37 Sperrung personenbezogener Daten aus ehemaligen Einrichtungen**

(1) Ist die Verarbeitung personenbezogener Daten aus ehemaligen Einrichtungen nach [§ 35 Abs. 1](#) nicht zulässig, sind diese Daten abweichend von [§ 19 Abs. 2](#) dem zuständigen öffentlichen Archiv zu übergeben. Daten, deren Speicherung nach Landesrecht unzulässig wäre, sind nach den Bestimmungen des [§ 4 Abs. 2 und 3](#) des Brandenburgischen Archivgesetzes zu behandeln.

(2) Abweichend von [§ 19 Abs. 3](#) dürfen gesperrte Daten nach Absatz 1 Satz 1 nur zur Behebung einer akuten Beweisnot, zu wissenschaftlichen Zwecken oder mit Zustimmung des Betroffenen weiterverarbeitet werden.

(3) Jeder Betroffene kann die Löschung rechtswidrig erhobener personenbezogener Daten fordern. Dem Antrag ist stattzugeben, soweit nicht schutzwürdige Belange der Öffentlichkeit oder Dritter dem entgegenstehen.

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

### **§ 38 Straftaten**

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, 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 bereithält, entschlüsselt, den Personenbezug herstellt oder löscht,
2. abrufen, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Übermittlung oder Weitergabe an sich oder andere veranlaßt,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Ebenso wird bestraft, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbar Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht. Der Versuch ist strafbar.

(2) Absatz 1 findet nur Anwendung, soweit die Tat nicht nach anderen Vorschriften mit Strafe bedroht ist.

### **§ 39 Ordnungswidrigkeiten**

(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 bereithält, entschlüsselt, den Personenbezug herstellt oder löscht,
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 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.

### **§ 40 Übergangsvorschriften**

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

(2) Für Behörden des Justizvollzuges gilt [§ 18](#) mit der Maßgabe, dass der Betroffene Auskunft oder Akteneinsicht erhält, soweit er zur Wahrnehmung seiner Rechte oder berechtigten Interessen auf die Kenntnis gespeicherter Daten angewiesen ist.

(3) Für personenbezogene Daten, die bereits automatisiert gespeichert sind, findet die Vorschrift des [§ 18 Abs. 2](#) erstmals in Fällen einer Veränderung oder Ergänzung des personenbezogenen Datensatzes Anwendung.

### **§ 40a Einschränkung von Grundrechten**

Das informationelle Selbstbestimmungsrecht nach [Artikel 11](#) Abs. 1 der Verfassung des Landes Brandenburg wird nach Maßgabe dieses Gesetzes eingeschränkt.

### **§ 41 (Inkrafttreten)<sup>1)</sup>**

---

<sup>1)</sup> Das Gesetz ist nach der erstmaligen Verkündung vom 22.01.1992 am 23.01.1992 in Kraft getreten.

---

## **Anlage 1**

### **Anforderungskatalog zu [§ 11a](#) Abs.1 Satz 3**

Werden Datenverarbeitungssysteme vor Ort oder über Datenfernübertragungseinrichtungen (Fernwartung) gewartet, so sind Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten geeignet sind,

1. sicherzustellen, dass nur dafür autorisiertes Personal die Wartung vornimmt;
2. sicherzustellen, dass jeder Wartungsvorgang nur mit Wissen und Willen der speichernden Stelle erfolgen kann;

3. zu verhindern, dass personenbezogene Daten im Rahmen der Wartung unbefugt entfernt oder übertragen werden;
4. sicherzustellen, dass alle Wartungsvorgänge während der Durchführung kontrolliert werden können;
5. sicherzustellen, dass alle Wartungsvorgänge nach der Durchführung nachvollzogen werden können;
6. zu verhindern, dass bei der Wartung Programme unbefugt aufgerufen werden können, die für die Wartung nicht benötigt werden;
7. zu verhindern, dass bei der Wartung Datenverarbeitungsprogramme unbefugt verändert werden können und
8. die Wartung so zu organisieren und zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

---

## **Anlage 2**

### **Mindestvertragsinhalt zu [§ 11a](#) Abs. 2 Satz 2**

In der schriftlichen Vereinbarung sind folgende Regelungen zu treffen:

1. Aussagen zu Art und Umfang der Wartung,
  2. Bestimmungen hinsichtlich der Abgrenzung der Rechte und Pflichten zwischen Auftraggeber und Auftragnehmer,
  3. eine Protokollierungspflicht beim Auftraggeber und die Verpflichtung des Auftragnehmers, Weisungen des Auftraggebers zum Umgang mit den Daten auszuführen und sich an dessen Weisungen zu halten,
  4. Regelung, dass die Daten ausschließlich für den Zweck der Wartung verwendet werden dürfen,
  5. Sicherstellung, dass keine Datenübermittlung an andere Stellen durch den Auftragnehmer erfolgt,
  6. nach Abschluß der Wartungsarbeiten sind die Daten zu löschen,
  7. die technische Verbindung muß vom Auftraggeber hergestellt werden; sofern dies nicht möglich ist, ist ein Rückrufverfahren verbindlich festzulegen,
  8. Anwesenheit des Systemverwalters ist möglichst sicherzustellen,
  9. Verschlüsselung von personenbezogenen Daten auf dem Übertragungsweg nach dem jeweiligen Stand der Technik und
  10. für den Fall, dass ein Auftragnehmer außerhalb der Mitgliedstaaten der Europäischen Union aus tätig wird, sind stets die jeweiligen Regelungen über die Übermittlung personenbezogener Daten an ausländische und internationale Stellen des [§ 17](#) anzuwenden.
-