Saarland

Saarländisches Gesetz zum Schutz personenbezogener Daten (Saarländisches Datenschutzgesetz - SDSG -)

Vom 24. März 1993 (Amtsbl. S. 286), zuletzt geändert durch § 72 des Gesetzes vom 27. Februar 2003 (Amtsbl. S. 498, 522))*

Inhaltsübersicht

* Dieses Gesetz dient der Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281, S. 31 ff.).

Erster Teil
Allgemeiner Datenschutz

Erster Abschnitt
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 Recht beeinträchtigt wird, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen (informationelles Selbstbestimmungsrecht).

§ 2
Anwendungsbereich

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch die Behörden und sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände sowie der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen). Als öffentliche Stellen gelten auch Vereinigungen ungeachtet ihrer Rechtsform, die Aufgaben öffentlicher Verwaltung wahrnehmen und an denen eine oder mehrere der in Satz 1 genannten Stellen mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen beteiligt sind; Gleiches gilt für weitere Beteiligungen dieser Vereinigungen. Nehmen nicht-öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes. Für den Landtag und für die Gerichte, den Rechnungshof sowie für die Behörden der Staats-

anwaltschaft gilt dieses Gesetz nur, soweit sie Verwaltungsaufgaben wahrnehmen; darüber hinaus gelten für die Behörden der Staatsanwaltschaft, soweit sie keine Verwaltungsaufgaben wahrnehmen, nur die Vorschriften des Zweiten Teils.

(2) Soweit öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, gelten für sie nur der Zweite Teil sowie der § 7 Abs. 1 und die §§ 9, 30 bis 32. Mit Ausnahme der Vorschriften über die Aufsichtsbehörde im Übrigen die die für nicht öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes einschließlich der Straf- und Bußgeldvorschriften anwendbar.

(3) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor. Im Übrigen gehen besondere Rechtsvorschriften, soweit sie auf die Verarbeitung personenbezogener Daten anzuwenden sind, den Vorschriften dieses Gesetzes vor.

(4) Amts- und Funktionsbezeichnungen dieses Gesetzes werden in weiblicher oder männlicher Form geführt.

§ 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 das Beschaffen von Daten über den Betroffenen,

2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,

3. Verändern das inhaltliche Umgestalten gespeicherter Daten,

4. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die verantwortliche Stelle weitergegeben oder zur Einsichtnahme bereitgehalten werden oder dass der Dritte zum Abruf in einem automatisierten Verfahren bereitgehaltene Daten abruft,

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

6. Löschen das Unkenntlichmachen gespeicherter Daten,

7. Nutzen jede sonstige Verwendung von Daten, ungeachtet der dabei angewendeten Verfahren.

(3) Verantwortliche Stelle ist jede der in § 2 Abs. 1 genannten Stellen, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.

(4) Empfänger ist jede Person oder Stelle, die personenbezogene Daten erhält.

(5) Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle, es sei denn, es handelt sich hierbei um den Betroffenen oder Stellen, die im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union personenbezogene Daten im Auftrag verarbeiten (§ 5).

(6) Automatisiert ist eine Datenverarbeitung, wenn sie durch Einsatz eines gesteuerten technischen Verfahrens selbsttätig abläuft.

(7) Eine Akte ist jede amtlichen oder dienstlichen Zwecken dienende Unterlage.

(8) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(9) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

1. die an den Betroffenen ausgegeben werden,
2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

§ 4
Zulässigkeit der Datenverarbeitung; Datenvermeidung und Datensparsamkeit

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

a) dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder

b) der Betroffene eingewilligt hat.

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 an Dritte über diese aufzuklären; er ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann.

(2) Die Verarbeitung personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben ist nur auf Grund einer besonderen Rechtsvorschrift zulässig. Dies gilt nicht, wenn

1. der Betroffene eingewilligt hat,

2. die Datenverarbeitung ausschließlich in seinem lebenswichtigen Interesse liegt und eine Einwilligung nicht oder nicht rechtzeitig eingeholt werden konnte,

3. die Angaben aus allgemein zugänglichen Quellen stammen und vom Betroffenen selbst offenbart wurden,

4. die Datenverarbeitung im Rahmen der Vorschriften der §§ 30, 31, 32 oder 33 dieses Gesetzes erforderlich ist,

5. ein rechtliches Interesse an der Verarbeitung der Daten besteht oder

6. die Datenverarbeitung zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Strafverfolgung erforderlich ist.

(3) Entscheidungen die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung seiner personenbezogenen Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Dies gilt nicht, wenn

1. eine Rechtsvorschrift dies ausdrücklich vorsieht,

2. damit dem Begehren des Betroffenen stattgegeben wird oder

3. dem Betroffenen die Tatsache einer Entscheidung nach Satz 1 mitgeteilt und ihm Gelegenheit gegeben wird, hierzu Stellung zu nehmen. Die verantwortliche Stelle ist verpflichtet, nach Eingang der Stellungnahme ihre Entscheidung erneut zu prüfen.

(4) Bei der Verarbeitung personenbezogener Daten haben sich die Art der Datenverarbeitung sowie die Auswahl und Gestaltung hierzu bestimmter technischer Einrichtungen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten.

§ 5
Verarbeitung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag einer öffentlichen Stelle verarbeitet, so bleibt sie verantwortliche Stelle im Sinne dieses Gesetzes. Der Auftragnehmer ist unter besonderer Berücksichtigung seiner Eignung sorgfältig auszuwählen. Der Auftrag ist schriftlich unter Festlegung von Gegenstand und Umfang der Datenverarbeitung zu erteilen. Er muss Weisungen zur Umsetzung der Vorgaben des § 11 enthalten. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen des vertraglich Festgelegten verarbeiten. Unterauftragsverhältnisse bedürfen ausdrücklicher Zustimmung. Der Auftraggeber hat

darauf zu achten, dass beim Auftragnehmer die nach § 11 Abs. 2 erforderlichen Maßnahmen getroffen sind.

(2) Soweit öffentliche Stellen personenbezogene Daten im Auftrag verarbeiten, gelten für sie nur die §§ 6, 7 Abs. 1, §§ 8, 11, 23, 26 bis 29, 35 und 36.

(3) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Bestimmungen dieses Gesetzes befolgt und sich der Kontrolle des Landesbeauftragten für Datenschutz unterwirft. Der Auftraggeber hat den Landesbeauftragten für Datenschutz über die Beauftragung zu unterrichten.

(4) Die Absätze 1 bis 3 gelten entsprechend für Personen und Stellen, die im Auftrag die Wartung und Betreuung von Anlagen und Verfahren zur automatisierten Datenverarbeitung wahrnehmen.

§ 6
Datengeheimnis

Denjenigen Personen, die bei öffentlichen Stellen oder ihren Auftragnehmern dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, solche Daten unbefugt zu verarbeiten; dies gilt auch nach Beendigung ihrer Tätigkeit. Diese Personen sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten.

§ 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 Geschäftsbereich die Ausführung der Rechtsvorschriften über den Datenschutz sicherzustellen. Verwaltungsvorschriften ergehen nach Anhörung des Landesbeauftragten für Datenschutz. Die Zuständigkeit der Fach- und Rechtsaufsichtsbehörden bleibt unberührt.

(2) Der erstmalige Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, bedarf hinsichtlich der in der Verfahrensbeschreibung festzulegenden Angaben (§ 9 Abs. 1) der schriftlichen Freigabe. In der Landesverwaltung ist die Freigabe durch diejenige oberste Landesbehörde zu erklären, die für die dem automatisierten Verfahren zugrunde liegende Rechtsmaterie federführend ist. Im Übrigen erfolgt die Freigabe durch die verantwortliche Stelle. Entsprechendes gilt für wesentliche Änderungen des Verfahrens. Vor der Entscheidung ist der Landesbeauftragte für Datenschutz zu hören.

§ 8
Behördlicher Datenschutzbeauftragter

(1) Öffentliche Stellen, die personenbezogene Daten verarbeiten, können einen behördlichen Datenschutzbeauftragten und einen Vertreter schriftlich bestellen. Diese müssen für ihre Tätigkeit geeignet sein, insbesondere über die erforderliche Zuverlässigkeit und Sachkunde verfügen. Die Bestellung externer Datenschutzbeauftragter ist zulässig, auch können mehrere öffentliche Stellen gemeinsam einen behördlichen Datenschutzbeauftragten bestellen, sofern die Aufgaben-

erfüllung hierdurch nicht beeinträchtigt wird. Der behördliche Datenschutzbeauftragte ist im Rahmen seiner Aufgabenerfüllung unmittelbar der Leitung der öffentlichen Stelle unterstellt. In Gemeinden und Gemeindeverbänden kann er auch einem hauptamtlichen Beigeordneten unterstellt werden. In seiner Funktion ist der behördliche Datenschutzbeauftragte weisungsfrei. Er kann sich unmittelbar an den Landesbeauftragten für Datenschutz wenden. Der behördliche Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Soweit erforderlich, ist er von anderen Tätigkeiten frei zu stellen und mit räumlichen, sachlichen und personellen Mitteln auszustatten.

(2) Der behördliche Datenschutzbeauftragte hat die verantwortliche Stelle bei der Ausführung datenschutzrechtlicher Vorschriften zu unterstützen und auf deren Einhaltung hinzuwirken. Zu den Aufgaben des behördlichen Datenschutzbeauftragten zählen insbesondere:

1. die nach § 9 zu erstellenden Verfahrensbeschreibungen zu führen,

2. die Vorabkontrolle nach § 11 Abs. 1 in Zusammenarbeit mit der verantwortlichen Stelle durchzuführen,

3. die verantwortliche Stelle bei dem Erarbeiten technischer und organisatorischer Maßnahmen nach § 11 Abs. 2 und 3 zu unterstützen und

4. die mit der Verarbeitung personenbezogener Daten befassten Personen mit den Bestimmungen dieses Gesetzes und anderer datenschutzrechtlicher Vorschriften vertraut zu machen.

Er kann zu seiner Aufgabenerfüllung jederzeit Einsicht in Datenbestände der verantwortlichen Stelle nehmen, soweit dem nicht gesetzliche Regelungen entgegen stehen. Soweit kein behördlicher Datenschutzbeauftragter bestellt ist, obliegt die Wahrnehmung von dessen Aufgaben der öffentlichen Stelle mit Ausnahme der Führung der Verfahrensverzeichnisse (Nummer 1) und der Durchführung der Vorabkontrolle

(Nummer 2). Die Führung des Verfahrensverzeichnisses und die Durchführung der Vorabkontrolle obliegen dem Landesbeauftragten für Datenschutz.

(3) Bedienstete der öffentlichen Stelle können sich in datenschutzrechtlichen Fragen jederzeit an den behördlichen Datenschutzbeauftragten wenden. Dieser ist verpflichtet, über die ihm bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder von Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der behördliche Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht durch den Betroffenen hiervon befreit wird.

§ 9
Verfahrensbeschreibung

(1) Die speichernde Stelle, die für den Einsatz eines automatisierten Verfahrens zuständig ist, ist verpflichtet, in einer Verfahrensbeschreibung folgende Angaben schriftlich festzulegen:

1. Name und Anschrift der verantwortlichen Stelle
2. die Bezeichnung des Verfahrens und seine Zweckbestimmungen, sowie die jeweiligen Rechtsgrundlagen,
3. die Art der verarbeiteten personenbezogenen Daten,
4. den Kreis der Betroffenen,
5. die Art regelmäßig zu übermittelnder personenbezogener Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten,

6. eine geplante Datenübermittlung in Drittländer,

7. Fristen für die Sperrung und Löschung der Daten,

8. die Ergebnisse der Vorabkontrolle nach § 11 Abs. 1,

9. die technischen und organisatorischen Maßnahmen nach § 11 Abs. 2,

10. die Technik der Verfahren, einschließlich Hard- und Software und

11. die zugriffsberechtigten Personen oder Personengruppen.

Änderungen sind dem behördlichen Datenschutzbeauftragten mitzuteilen. Soweit speichernde und verantwortliche Stelle nicht identisch sind, ist diese Verfahrensbeschreibung und deren Änderungen auch dem behördlichen Datenschutzbeauftragten der verantwortlichen Stelle zur Verfügung zu stellen.

(2) Die Angaben der Verfahrensbeschreibung können bei dem behördlichen Datenschutzbeauftragten der verantwortlichen Stelle von jedermann eingesehen werden. Dies gilt jedoch insbesondere für die Angaben zu den Nummern 8, 9 und 10 nur, soweit hierdurch die Sicherheit des Verfahrens nicht beeinträchtigt wird. Satz 1 gilt nicht für

1. Verfahren des Landesamtes für Verfassungsschutz,

2. Verfahren zum Zwecke der Gefahrenabwehr und der Strafverfolgung,

3. Verfahren der Steuerfahndung,

4. Verfahren der öffentlich-rechtlichen Unternehmen, die am Wettbewerb teilnehmen,

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

(3) Soweit eine verantwortliche Stelle keinen behördlichen Datenschutzbeauftragten bestellt hat, tritt an dessen Stelle der Landesbeauftragte für Datenschutz.

§ 10
Automatisiertes Abrufverfahren

(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.

(2) Die Staatskanzlei und die Ministerien werden ermächtigt, für ihren Geschäftsbereich automatisierte Abrufverfahren durch Rechtsverordnung zuzulassen, 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 Abrufs sind festzulegen. Der Landesbeauftragte für Datenschutz ist vorher zu hören.

(3) Die am Abrufverfahren beteiligten Stellen haben die nach § 11 Abs. 2 erforderlichen Maßnahmen zu treffen.

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

(5) Personenbezogene Daten dürfen für Stellen außerhalb des öffentlichen Bereichs zum automatisierten Abruf nicht bereitgehalten werden.

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

(7) Die Absätze 1 bis 6 gelten entsprechend für die Einrichtung gemeinsamer oder verbundener automatisierter Verfahren, in und aus denen mehrere öffentliche Stellen personenbezogene Daten verarbeiten sollen. Die Beteiligten bestimmen eine nach diesem Gesetz verantwortliche Stelle und legen schriftlich den jeweiligen Verantwortungsbereich fest.

§ 11
Vorabkontrolle; technische und organisatorische Maßnahmen

(1) Vor dem erstmaligen Einsatz automatisierter Verfahren ist zu prüfen, welche Gefahren hierdurch für das informationelle Selbstbestimmungsrecht erwachsen können (Vorabkontrolle). Automatisierte Verfahren dürfen nur dann eingesetzt werden, wenn sichergestellt ist, dass keine Gefahren bestehen oder diese durch Maßnahmen nach Absatz 2 verhindert werden können. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist.

(2) Werden personenbezogene Daten automatisiert verarbeitet, ist die innerbehördliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigen ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, und dass diese Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

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

Zweiter Abschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 12
Erhebung; Benachrichtigung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Personenbezogene Daten sind grundsätzlich bei dem Betroffenen mit dessen Kenntnis zu erheben. Dieser ist über den Verwendungszweck aufzuklären. Werden personenbezogene Daten auf Grund einer Rechtsvorschrift erhoben, ist diese anzugeben und zu erläutern. Soweit eine Auskunftspflicht besteht oder die Angaben Voraussetzung für die Gewährung von Rechtsvorteilen sind, ist der Betroffene hierauf, ansonsten auf die Freiwilligkeit seiner Angaben, hinzuweisen.

(2) Das Erheben personenbezogener Daten bei dem Betroffenen ohne dessen Kenntnis ist nur zulässig, wenn Bundes- oder Landesrecht dies erlaubt oder der Schutz von Leben und Gesundheit dies gebietet.

(3) Bei öffentlichen Stellen dürfen personenbezogene Daten ohne Kenntnis des Betroffenen nur unter den in § 13 Abs. 2 Satz 1 Buchstaben b bis g genannten Voraussetzungen erhoben werden. Im Falle des § 13 Abs. 2 Satz 1 Buchstabe d ist der Betroffene darauf hinzuweisen, wo die Daten erhoben werden können.

(4) Bei Dritten außerhalb des öffentlichen Bereichs dürfen personenbezogene Daten ohne Kenntnis des Betroffenen nur unter den Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstaben c, e und g erhoben werden. Auf Verlangen des Dritten ist dieser über den Verwendungszweck aufzuklären. Auf eine Auskunftsverpflichtung, ansonsten auf die Freiwilligkeit der Angaben, ist hinzuweisen.

(5) Werden personenbezogene Daten ohne Kenntnis des Betroffenen erhoben, ist dieser von der Datenerhebung zu benachrichtigen, sofern die Aufgabenerfüllung hierdurch nicht beeinträchtigt ist. Im Falle einer beabsichtigten Übermittlung hat die Benachrichtigung spätestens mit deren Durchführung zu erfolgen, sofern die Aufgabenerfüllung hierdurch nicht beeinträchtigt ist. Die Benachrichtigung umfasst zumindest die Angabe des Verwendungszwecks und der Rechtsgrundlage sowie einen Hinweis auf die Rechte des Betroffenen nach dem dritten Abschnitt. Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. die Verarbeitung ausdrücklich durch Rechtsvorschrift vorgesehen ist,

2. Betroffene auf andere Weise Kenntnis von der Verarbeitung ihrer Daten erlangt haben oder

3. die Benachrichtigung nicht möglich ist oder mit einen unverhältnismäßig hohem Aufwand verbunden wäre.

§ 13
Speicherung, Veränderung und Nutzung; Zweckbindung

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

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

a) der Betroffene eingewilligt hat,

b) 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 Zwecks seine Einwilligung erteilen würde,

c) eine Rechtsvorschrift dies erlaubt oder zwingend voraussetzt,

d) Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

e) es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder unmittelbar drohender Gefahren für Leben, Gesundheit oder persönliche Freiheit anderer erforderlich ist,

f) sie aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde Stelle sie veröffentlichen dürfte, es sei denn, dass das berechtigte Interesse des Betroffenen an dem Ausschluss der Zweckänderung der gespeicherten Daten offensichtlich überwiegt,

g) es zu Zwecken einer öffentlichen Auszeichnung oder Ehrung des Betroffenen erforderlich ist oder

h) sich bei Gelegenheit der Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheint.

Berufs- oder besondere Amtsgeheimnisse bleiben unberührt.

(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. Zulässig ist auch die Verarbeitung zu Ausbildungs- und

Prüfungszwecken, soweit nicht berechtigte Interessen des Betroffenen an der Geheimhaltung der Daten überwiegen.

§ 14
Übermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich ist und die Voraussetzungen des § 13 Abs. 1 Satz 2 oder Satz 3 oder des Absatzes 2 vorliegen sowie zur Wahrnehmung von Aufgaben nach § 13 Abs. 3.

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

(3) Die Verantwortung für die 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 (§ 10), so trägt die Verantwortung für die Rechtmäßigkeit des Abrufs 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
Zugriffs- und Informationsrecht des Landtages

(1) Der Landtag hat das Recht des unmittelbaren Zugriffs auf die Daten, die von den in § 2 Abs. 1 genannten Behörden automatisiert verarbeitet werden. Das Zugriffsrecht kann auch für den Präsidenten des Landtages, die Fraktionen und die einzelnen Mitglieder des Landtages in Anspruch genommen werden.

(2) Personenbezogene Daten unterliegen nicht dem Zugriffsrecht. Das Zugriffsrecht ist ausgeschlossen, wenn dem Zugriff ein gesetzliches Verbot oder zwingende Geheimhaltungsgründe entgegenstehen.

(3) Die Behörden des Landes sind verpflichtet, in den Grenzen des Absatzes 2 dem Landtag, dem Präsidenten des Landtages, den Fraktionen und einzelnen Mitgliedern des Landtages die von diesen verlangten Auskünfte aufgrund automatisierter Verfahren zu geben, soweit Programme zur Verwertung vorhanden sind.

(4) Der Landtag kann durch seinen Präsidenten von der Landesregierung Auskünfte über die Verfahren zur automatisierten Datenverarbeitung verlangen, auf die sich das Zugriffsrecht des Absatzes 1 und das Auskunftsrecht des Absatzes 3 erstreckt. Das Auskunftsrecht kann umfassen:

1. Name des Verfahrens mit kurzer Funktionsbeschreibung,
2. Aufbau der Datensätze mit Angaben über den Inhalt und die Ordnungskriterien,
3. vorhandene Auswertungsprogramme,
4. zuständige Behörde.

§ 16
Übermittlung an Personen oder Stellen außerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs ist zulässig, wenn

a) die zur Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist und die Voraussetzungen des § 13 Abs. 1 Satz 2 oder Satz 3 vorliegen,

b) die Voraussetzungen des § 13 Abs. 2 Satz 1 Buchstaben a, c, e, f oder vorliegen, , wobei § 13 Abs. 2 Satz 2 unberührt bleibt,

c) der Auskunftsbegehrende 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.

In den Fällen des Satzes 1 Buchstabe d ist der Betroffene über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise zu unterrichten.

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

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

§ 17
Übermittlung an Stellen außerhalb der Bundesrepublik Deutschland

(1) Für die Übermittlung personenbezogener Daten an öffentliche Stellen der Mitgliedstaaten der Europäischen Union sowie anderer Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder an Organe und Einrichtungen der Europäischen Union gelten die §§ 14 und 30; für die Übermittlung an nicht öffentliche Stellen gilt § 16 entsprechend.

(2) Die Übermittlung personenbezogener Daten an Stellen außerhalb der Mitgliedstaaten der Europäischen Union ist nur zulässig, wenn beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist. Zu der Frage, ob das Datenschutzniveau angemessen ist, muss der Landesbeauftragte für Datenschutz gehört werden.

(3) Ist ein angemessenes Datenschutzniveau nicht gewährleistet, dürfen personenbezogene Daten nur übermittelt werden, wenn

1. der Betroffene eingewilligt hat,
2. die Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist,
3. die Übermittlung zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,
4. die Übermittlung für die Erfüllung eines Vertrages zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,
5. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrages erforderlich ist, der im Interesse des Betroffenen von der verant-

wortlichen Stelle geschlossen wurde oder geschlossen werden soll oder

6. die Daten aus einem Register entnommen wurden, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, offen steht, soweit die gesetzlichen Voraussetzungen zur Einsichtnahme im Einzelfall gegeben sind.

(4) Datenempfänger sind darauf hinzuweisen, dass die Daten nur zu den Zwecken verarbeitet werden dürfen, für die sie übermittelt wurden.

(5) Die Verantwortung für die Zulässigkeit von Datenübermittlungen nach den Absätzen 2 und 3 trägt die übermittelnde Stelle.

§ 18
Mobile Speicher- und Verarbeitungsmedien

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, 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 §§ 20 bis 24 ausüben kann, und

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

unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

Dritter Abschnitt
Rechte des Betroffenen

§ 19
Unabdingbarkeit der Rechte des Betroffenen

Die in den §§ 20 bis 24 aufgeführten Rechte können durch Rechtsgeschäft weder ausgeschlossen noch beschränkt werden.

§ 20
Auskunft

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

1. die zu seiner Person gespeicherten Daten,
2. den Zweck und die Rechtsgrundlage der Verarbeitung sowie
3. die Herkunft der Daten und die Empfänger von Übermittlungen, soweit dies gespeichert ist.

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

(2) In dem Antrag soll die Art der Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung nach pflichtgemäßem Ermessen; sind die Daten in Akten gespeichert, ist dem Betroffenen auf Verlangen Einsicht zu gewähren. Auskunft aus Akten oder Akteneinsicht sind zu gewähren, soweit der Betroffene An-

gaben macht, die das Auffinden der Daten mit angemessenem Aufwand ermöglichen, und soweit sich aus § 29 Saarländisches Verwaltungsverfahrensgesetz nichts anderes ergibt.

(3) Die Verpflichtung zur Auskunftserteilung oder zur Gewährung der Akteneinsicht entfällt, soweit

a) dies die ordnungsgemäße Erfüllung der Aufgaben der verantwortlichen Stelle gefährden würde,

b) dies die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

c) die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen der berechtigten Interessen eines Dritten, geheimgehalten werden müssen.

(4) Einer Begründung für die Verweigerung der Auskunft oder Akteneinsicht 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. Der Betroffene ist in jedem Fall darauf hinzuweisen, dass er sich an den Landesbeauftragten für Datenschutz wenden kann.

(5) Bezieht sich die Auskunftserteilung oder die Akteneinsicht auf die Herkunft personenbezogener Daten von Behörden des Verfassungsschutzes, der Staatsanwaltschaft und der Polizei, von Finanzbehörden, 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 Bundesdatenschutzgesetz 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 3 und 4 entsprechend.

§ 21
Berichtigung, Sperrung und Löschung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Sind personenbezogene Daten, die nicht automatisiert verarbeitet werden, 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 sperren, wenn

a) ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt,

b) eine Löschung nach Absatz 3 Satz 2 nicht in Betracht kommt und der Betroffene die Sperrung beantragt,

c) der Betroffene an Stelle der Löschung nach Absatz 3 Satz 1 Buchstabe a die Sperrung beantragt,

d) wenn Grund zu der Annahme besteht, dass durch die Löschung der Daten berechtigte Interessen des Betroffenen beeinträchtigt werden,

e) sie nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind oder

f) sie auf Grund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen.

In den Fällen nach Satz 1 Buchstabe d sind die Gründe aufzuzeichnen. Bei automatisierten Verfahren 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 zur Behebung einer bestehenden Beweisnot oder aus sonstigen

im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist oder der Betroffene eingewilligt hat.

(3) Personenbezogene Daten sind zu löschen, wenn

a) ihre Speicherung unzulässig ist oder

b) ihre Kenntnis für die verantwortliche 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; soweit hiernach eine Löschung nicht in Betracht kommt, sind die Daten auf Antrag des Betroffenen zu sperren.

(4) Abgesehen von den Fällen des Absatzes 3 Satz 1 Buchstabe a ist von einer Löschung abzusehen, soweit die gespeicherten Daten aufgrund von Rechtsvorschriften einem Archiv zur Übernahme anzubieten oder von einem Archiv zu übernehmen sind.

(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.

§ 22
Einwendungsrecht des Betroffenen

Betroffene können gegenüber der verantwortlichen Stelle auch gegen eine durch Rechtsvorschrift erlaubte Verarbeitung ihrer personenbezo-

genen Daten unter Hinweis auf ein schutzwürdiges besonderes persönliches Interesse im Einzelfall schriftlich Einwände vorbringen. In diesen Fällen bleibt die Verarbeitung nur dann zulässig, wenn eine Prüfung ergibt, dass das öffentliche Interesse an der Verarbeitung überwiegt. Betroffene sind über das Ergebnis der Prüfung schriftlich zu unterrichten. Wird dem Einwand nicht entsprochen, ist der Betroffenen darauf hinzuweisen, dass er sich an den Landesbeauftragten für Datenschutz wenden kann. Das Einwendungsrecht besteht nicht, wenn eine Rechtsvorschrift zur Verarbeitung verpflichtet.

§ 23
Anrufungsrecht des Betroffenen

(1) Jedermann hat das Recht, sich unmittelbar an den Landesbeauftragten für Datenschutz 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.

(2) Niemand darf deswegen benachteiligt oder gemaßregelt werden, weil er sich an den Landesbeauftragten für Datenschutz wendet.

§ 24
Schadensersatz

(1) Wird dem Betroffenen durch eine nach den Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung seiner personenbezogenen Daten ein Schaden zugefügt, so ist die verantwortliche 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 nach den Sätzen 1 und 2 für jedes schädigende Ereignis bis zu einem Betrag von 125 000 Euro.

(2) Soweit die unzulässige oder unrichtige Verarbeitung personenbezogener Daten nicht automatisiert erfolgt, haftet die verantwortliche Stelle nur bei Verschulden. Die verantwortliche Stelle haftet nicht, wenn sie nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihr nicht zur Last gelegt werden kann.

(3) Auf das Mitverschulden des Betroffenen und auf die Verjährung des Entschädigungsanspruchs sind die §§ 254, 839 Abs. 3 und 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(4) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

Zweiter Teil
Landesbeauftragter für Datenschutz

§ 25
Berufung und Rechtsstellung

(1) Der Landtag wählt auf Vorschlag der Landesregierung einen Landesbeauftragten für Datenschutz. Dieser muss die Befähigung zum Richteramt oder zum höheren Verwaltungsdienst haben.

(2) Der Landesbeauftragte für Datenschutz wird auf die Dauer von sechs Jahren in ein Beamtenverhältnis auf Zeit berufen. Er wird vom Präsidenten des Landtages ernannt. Nach Beendigung seiner Amtszeit führt der Landesbeauftragte für Datenschutz die Amtsgeschäfte bis zur Ernennung seines Nachfolgers fort, längstens jedoch für sechs Monate nach Ablauf seiner Amtszeit.

(3) Der Landesbeauftragte für Datenschutz wird dem Landtag angegliedert. Er ist in Erfüllung seines Auftrages nach diesem Gesetz an Weisungen nicht gebunden. Der Landesbeauftragte für Datenschutz untersteht der Dienstaufsicht des Präsidenten des Landtages nur, soweit seine Unabhängigkeit nicht beeinträchtigt wird.

(4) Dem Landesbeauftragten für Datenschutz sind das zur Erfüllung seiner Aufgaben notwendige Personal und die notwendigen Sachmittel zur Verfügung zu stellen. Das ihm zur Erfüllung seiner Aufgaben zugewiesene Personal ist nur an seine Weisungen gebunden. Die Zuweisung des Personals erfolgt im Benehmen mit dem Landesbeauftragten für Datenschutz.

(5) Der Landesbeauftragte für Datenschutz bestellt einen Mitarbeiter zum Stellvertreter. Der Stellvertreter führt die Geschäfte, wenn der Landesbeauftragte für Datenschutz an der Ausübung des Amtes verhindert ist. Absatz 1 Satz 2 gilt entsprechend.

(6) Der Landesbeauftragte für Datenschutz ist verpflichtet, über die ihm amtlich bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

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

§ 26
Aufgaben

(1) Der Landesbeauftragte für Datenschutz überwacht bei den in § 2 Abs. 1 genannten Stellen und den Stellen, die sich gemäß § 5 Abs. 3 oder § 30 Abs. 7 seiner Kontrolle unterworfen haben, die Einhaltung der Vorschriften über den Datenschutz.

(2) Der Landesbeauftragte für Datenschutz kann Empfehlungen zur Verbesserung des Datenschutzes geben, insbesondere kann er die für die Sicherstellung des Datenschutzes zuständigen Stellen (§ 7 Abs. 1) in Fragen des Datenschutzes beraten. 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 des Landtages oder des für den Datenschutz zuständigen Landtagsausschusses kann der Landesbeauftragte für Datenschutz ferner Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenbereich unmittelbar betreffen, nachgehen.

(4) Der Landtag und die Landesregierung können den Landesbeauftragten für Datenschutz mit der Erstattung von Gutachten und Stel-

lungnahmen oder der Durchführung von Untersuchungen in Datenschutzfragen betrauen.

(5) Der Landesbeauftragte für Datenschutz 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, zusammen.

§ 27
Beanstandungen durch den Landesbeauftragten

(1) Stellt der Landesbeauftragte für Datenschutz Verstöße gegen Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, teilt er der verantwortlichen Stelle das Ergebnis seiner Kontrolle mit. Mit der Mitteilung kann er Vorschläge zur Beseitigung festgestellter Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden. Erhebliche Verstöße beanstandet er

1. bei der Landesverwaltung gegenüber der zuständigen obersten Landesbehörde,

2. bei den Gemeinden und Gemeindeverbänden sowie den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen gegenüber dem vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. Im Falle von Satz 3 Nr. 2 unterrichtet der Landesbeauftragte für Datenschutz gleichzeitig auch die zuständige Aufsichtsbehörde.

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

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

§ 28
Durchführung der Kontrolle

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

1. Auskunft auf die Fragen zu erteilen sowie Einsicht in alle Vorgänge und Aufzeichnungen zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,

2. jederzeit - auch unangemeldet - ungehinderten Zutritt zu allen Diensträumen zu gewähren.

(2) Die Rechte nach Absatz 1 dürfen nur von dem Landesbeauftragten für Datenschutz persönlich ausgeübt werden, wenn die oberste Landesbehörde im Einzelfall feststellt, dass die Sicherheit des Bundes oder eines Landes dies gebietet. In diesem Fall müssen personenbezogene Daten eines Betroffenen, dem von der datenverarbeitenden Stelle Vertraulichkeit besonders zugesichert worden ist, auch ihm gegenüber nicht offenbart werden.

§ 29
Tätigkeitsberichte

Der Landesbeauftragte für Datenschutz legt dem Landtag und der Landesregierung jeweils für zwei Kalenderjahre einen Bericht über seine Tätigkeit vor. Die Landesregierung legt hierzu ihre Stellungnahme dem Landtag vor. Diese soll innerhalb von sechs Monaten nach Vorlage des Tätigkeitsberichts dem Landtag zugeleitet werden. § 25 Abs. 7 bleibt unberührt.

Dritter Teil
Besonderer Datenschutz

§ 30
Datenverarbeitung zum Zwecke wissenschaftlicher Forschung

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

(2) Öffentliche Stellen dürfen personenbezogene Daten ohne Einwilligung des Betroffenen für ein bestimmtes Forschungsvorhaben verarbeiten, wenn dessen schutzwürdige Belange wegen der Art der Daten und ihrer Verwendung oder wegen ihrer Offenkundigkeit nicht beeinträchtigt werden. Der Einwilligung des Betroffenen bedarf es auch nicht, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Soweit Stellen des Landes personenbezogene Daten übermitteln, bedarf die Übermittlung der vorherigen Genehmigung der obersten Landesbehörde oder einer von dieser bestimmten Stelle. Im Übrigen entscheidet der Behördenleiter. Die Genehmigung muss den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Landesbeauftragten für Datenschutz mitzuteilen.

(4) Die Daten sind, sobald der Forschungszweck es gestattet, zu anonymisieren. Ist dies nicht möglich, sind sie zu pseudonymisieren. Die Merkmale, mit deren Hilfe der Personenbezug wieder hergestellt werden kann, sind gesondert zu speichern; sie sind zu löschen, sobald der Forschungszweck dies gestattet.

(5) Soweit nach Absatz 2 Daten übermittelt wurden, dürfen diese nur mit Einwilligung des Betroffenen weiter übermittelt oder für einen anderen als den ursprünglichen Zweck verarbeitet werden.

(6) 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.

(7) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen diesem personenbezogene Daten nur übermittelt werden, wenn er sich verpflichtet, die Vorschriften der Absätze 4 - 6 einzuhalten und sich der Kontrolle des Landesbeauftragten für Datenschutz unterwirft. Die übermittelnde Stelle unterrichtet den Landesbeauftragten für Datenschutz.

§ 31
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 Bereichs nur zulässig, wenn der Betroffene eingewilligt hat, der Empfänger ein rechtliches Interesse glaubhaft macht oder der Dienstverkehr es erfordert. Die Datenübermittlung an

einen künftigen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung des Betroffenen zulässig.

(2) Die Verarbeitung 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; § 21 Abs. 3 Satz 2 und Absatz 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 § 11 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.

§ 32
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 eine 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. Dies gilt nicht, wenn ein Gesetz die anderweitige Verarbeitung dieser Daten zulässt oder wenn diese Daten zur Abwehr erheblicher Nachteile für das Gemeinwohl oder unmittelbar drohender Gefahren für Leben, Gesundheit oder persönliche Freiheit anderer erforderlich sind. Die Daten sind zu löschen, sobald sie zur Erfüllung dieser Zwecke nicht mehr benötigt werden.

§ 33
Öffentlich-rechtliche Religionsgesellschaften

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften ist in entsprechender Anwendung des § 14 zulässig, sofern sichergestellt ist, dass bei dem Empfänger ausreichende Datenschutzmaßnahmen getroffen sind.

§ 34
(gestrichen)

Vierter Teil
Straf- und Bußgeldvorschriften; Übergangsvorschriften

§ 35
Straftaten

(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind, gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen,

1. erhebt, speichert, verändert, weitergibt, zur Einsichtnahme oder zum Abruf bereithält, löscht oder nutzt,

2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst,

wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

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

§ 36
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, verändert, weitergibt, zur Einsichtnahme oder zum Abruf bereithält, löscht oder nutzt,

2. abruft, einsieht, sich verschafft oder durch Vortäuschung falscher Tatsachen ihre Weitergabe an sich oder andere veranlasst.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50.000 Euro geahndet werden.

§ 37
Übergangsvorschriften

(1) überholt

(2) Soweit landesrechtliche Vorschriften noch den Begriff „Datei“ verwenden, ist Datei

1. eine Sammlung von Daten, die ohne Rücksicht auf die Art der Speicherung durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei) oder

2. eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht automatisierte Datei).

§ 38
Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.