

Amtliche Abkürzung:	LDSG	Quelle:	
Neugefasst durch	18.09.2000	Fundstelle:	GBI. 2000, 648
Bek. vom:		Gliede-	2040
Textnachweis ab:	01.01.2005	rungs-Nr:	
Dokumenttyp:	Gesetz		

**Gesetz zum Schutz personenbezogener Daten
(Landesdatenschutzgesetz - LDSG)
in der Fassung vom 18. September 2000**

Zum 05.10.2016 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: letzte berücksichtigte Änderung: § 8a eingefügt sowie Inhaltsübersicht angepasst durch Artikel 2 des Gesetzes vom 17. Dezember 2015 (GBI. S. 1191, 1198)

Inhaltsübersicht

ERSTER ABSCHNITT

Allgemeine Bestimmungen

Aufgabe des Gesetzes	§ 1
Anwendungsbereich	§ 2
Begriffsbestimmungen	§ 3
Zulässigkeit der Datenverarbeitung	§ 4
Rechte des Betroffenen	§ 5
Datengeheimnis	§ 6
Verarbeitung personenbezogener Daten im Auftrag	§ 7
Automatisiertes Abrufverfahren	§ 8
Gemeinsame Verfahren	§ 8a
Technische und organisatorische Maßnahmen	§ 9
Behördlicher Datenschutzbeauftragter	§ 10
Verfahrensverzeichnis	§ 11
Vorabkontrolle	§ 12

ZWEITER ABSCHNITT

Rechtsgrundlagen der Datenverarbeitung

Erhebung	§ 13
Unterrichtung bei der Erhebung	§ 14
Speicherung, Veränderung und Nutzung	§ 15
Übermittlung an Stellen innerhalb des öffentlichen Bereichs	§ 16
Übermittlung an Stellen der öffentlich-rechtlichen Religionsgesellschaften	§ 17
Übermittlung an Stellen außerhalb des öffentlichen Bereichs	§ 18
Übermittlung für Zwecke der wissenschaftlichen Forschung	§ 19
Übermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes	§ 20
Videobeobachtung und Videoaufzeichnung (Videoüberwachung)	§ 20a

DRITTER ABSCHNITT

Rechte des Betroffenen

Auskunft	§ 21
Berichtigung	§ 22
Löschung	§ 23
Sperrung	§ 24

Schadensersatz	§ 25
VIERTER ABSCHNITT	
Landesbeauftragter für den Datenschutz	
Bestellung und Rechtsstellung	§ 26
Anrufung des Landesbeauftragten für den Datenschutz	§ 27
Kontrolle durch den Landesbeauftragten für den Datenschutz	§ 28
Pflicht zur Unterstützung	§ 29
Mitteilung des Ergebnisses der Kontrolle, Beanstandungen	§ 30
Weitere Aufgaben des Landesbeauftragten für den Datenschutz	§ 31
Meldung an den Landesbeauftragten für den Datenschutz	§ 32
Gebühren für Amtshandlungen im nichtöffentlichen Bereich	§ 32a
FÜNFTER ABSCHNITT	
Besondere Bestimmungen	
Verarbeitung besonderer Arten personenbezogener Daten	§ 33
Datenverarbeitung in der gemeinsamen Dienststelle	§ 33a
Zweckbindung bei der Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen	§ 34
Verarbeitung personenbezogener Daten durch Forschungseinrichtungen	§ 35
Datenverarbeitung bei Dienst- und Arbeitsverhältnissen	§ 36
Verarbeitung personenbezogener Daten durch den Südwestrund	§ 37
Rundfunkbeauftragter für den Datenschutzfunk	§ 38
SECHSTER ABSCHNITT	
Übergangs- und Schlussvorschriften	
<i>(aufgehoben)</i>	§ 39
Ordnungswidrigkeiten	§ 40
Straftaten	§ 41
aufgehoben	§ 42
Änderung des Landesverwaltungsverfahrensgesetzes	§ 43
Änderung des Vermessungsgesetzes	§ 44
Änderung des Landeskatastrophenschutzgesetzes	§ 45
Änderung des Feuerwehrgesetzes	§ 46
Änderung des Gesetzes zu dem Staatsvertrag über Bildschirmtext	§ 47
Änderung des Meldegesetzes	§ 48
Inkrafttreten	§ 49

ERSTER ABSCHNITT

Allgemeine Bestimmungen

§ 1

Aufgabe des Gesetzes

Aufgabe dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch die Verarbeitung seiner personenbezogenen Daten durch öffentliche Stellen in seinem Persönlichkeitsrecht beeinträchtigt wird.

§ 2

Anwendungsbereich

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen). Einzelne Vorschriften gelten auch für die Tätigkeit des Landesbeauftragten für den Datenschutz im nichtöffentlichen Bereich.

(2) Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen beteiligt sind. Beteiligt sich eine juristische Person oder sonstige

Vereinigung des privaten Rechts, auf die dieses Gesetz nach Satz 1 Anwendung findet, an einer weiteren Vereinigung des privaten Rechts, so findet Satz 1 entsprechende Anwendung. Nehmen nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes.

(3) Dieses Gesetz gilt für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird; § 9 findet auch dann Anwendung, wenn der Landtag bei der Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeitet. Die §§ 10, 11, 27 bis 32 gelten für die Gerichte nur, soweit sie in Verwaltungsangelegenheiten tätig werden, für den Rechnungshof und die staatlichen Rechnungsprüfungsämter nur außerhalb ihrer Prüfungstätigkeit.

(4) Soweit öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, sind die für nichtöffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes entsprechend anzuwenden. Satz 1 gilt nicht für Zweckverbände.

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

§ 3 **Begriffsbestimmungen**

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

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

1. Erheben das Beschaffen von personenbezogenen Daten über den Betroffenen,
2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von personenbezogenen Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung,
3. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
4. Übermitteln das Bekanntgeben personenbezogener Daten an einen Dritten in der Weise, dass
 - a) die Daten an den Dritten weitergegeben werden oder
 - b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
5. Nutzen jede sonstige Verwendung personenbezogener Daten innerhalb der Daten verarbeitenden Stelle,
6. Sperren die Einschränkung der weiteren Verarbeitung personenbezogener Daten,
7. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(3) Verantwortliche Stelle ist jede Stelle, die personenbezogene Daten für sich selbst verarbeitet oder durch andere im Auftrag verarbeiten lässt.

(4) Empfänger ist jede Person oder Stelle, die Daten erhält, mit Ausnahme des Betroffenen.

(5) Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle, ausgenommen der Betroffene sowie diejenige Person und Stelle, die in einem Mitgliedstaat der Europäischen Union personenbezogene Daten im Auftrag verarbeitet.

(6) Anonymisieren ist das Verändern personenbezogener Daten in der Weise, dass Einzelangaben über persönliche und sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmaren natürlichen Person zugeordnet werden können.

(7) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(8) Automatisiert ist eine Datenverarbeitung, wenn sie durch Einsatz eines elektronischen Datenverarbeitungssystems programmgesteuert durchgeführt wird.

(9) Eine Datei ist:

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

(10) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage. Nicht hierunter fallen Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

§ 4

Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig,

1. wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder
2. soweit der Betroffene eingewilligt hat.

(2) Wird die Einwilligung beim Betroffenen eingeholt, ist er über die beabsichtigte Datenverarbeitung und den Zweck der Verarbeitung aufzuklären. Die Aufklärungspflicht umfasst bei einer beabsichtigten Übermittlung auch den Empfänger der Daten. Über die Möglichkeit einer weitergehenden Datenverarbeitung auf Grund gesetzlicher Bestimmungen ist er zu unterrichten. Der Betroffene ist unter Darlegung der Folgen darauf hinzuweisen, dass er die Einwilligung verweigern kann und dass die Möglichkeit besteht, die Einwilligung zu widerrufen.

(3) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

(4) Die Einwilligung kann auch elektronisch erklärt werden, wenn die empfangende Stelle sicherstellt, dass

1. die Einwilligung nur durch eine eindeutige und bewusste Handlung des Einwilligenden erfolgen kann,
2. sie nicht unerkennbar verändert werden kann,
3. ihr Urheber eindeutig erkannt werden kann und
4. die Einwilligung (Tag, Uhrzeit, Inhalt) protokolliert wird.

§ 3a des Landesverwaltungsverfahrensgesetzes findet auf die Einwilligung keine Anwendung.

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

(6) Der Betroffene hat das Recht, gegenüber der Verarbeitung seiner Daten, auch wenn diese rechtmäßig ist, ein schutzwürdiges, in seiner persönlichen Situation begründetes Interesse einzuwenden (Einwendungsrecht). Die Verarbeitung ist in diesem Fall nur zulässig, wenn eine Abwägung ergeben hat, dass sein Interesse hinter dem öffentlichen Interesse an der Verarbeitung zurückzustehen hat. Das Ergebnis der Abwägung ist ihm unter Angabe der Gründe mitzuteilen. Sätze 1 bis 3 finden keine Anwendung in den in § 33 Abs. 3 genannten Fällen.

(7) Entscheidungen, die für den Betroffenen eine nachteilige rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht auf eine Bewertung seiner Persönlichkeitsmerkmale gestützt werden, die ausschließlich im Wege einer automatisierten Verarbeitung seiner personenbezogenen Daten zustande gekommen ist.

§ 5 Rechte des Betroffenen

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

1. Auskunft über die zu seiner Person gespeicherten Daten (§ 21),
2. Berichtigung, Löschung und Sperrung der zu seiner Person gespeicherten Daten (§§ 22 bis 24),
3. Auskunft aus dem Verzeichnisse (§ 11 Abs. 4),
4. Einwendung eines schutzwürdigen, in seiner persönlichen Situation begründeten Interesses gegenüber der Verarbeitung seiner Daten (§ 4 Abs. 6),
5. Schadensersatz (§ 25),
6. Anrufung des Landesbeauftragten für den Datenschutz (§ 27).

Diese Rechte können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Wird für den Erhalt einer Leistung, das Erkennen einer Person oder für einen anderen Zweck ein Datenträger herausgegeben, den der Inhaber mit sich führen kann und auf dem seine personenbezogenen Daten automatisiert verarbeitet werden, hat die verantwortliche Stelle sicherzustellen, dass er dies erkennen und seine ihm nach Absatz 1 Nr. 1 bis 6 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.

§ 6 Datengeheimnis

Den bei öffentlichen Stellen beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder sonst zu verwenden (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 7 Verarbeitung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag öffentlicher Stellen durch andere Personen oder Stellen verarbeitet, bleibt der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in § 5 Abs. 1 Satz 1 Nr. 1 bis 5 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftraggeber hat den Auftragnehmer sorgfältig auszuwählen. Dabei ist besonders zu berücksichtigen, ob der Auftragnehmer ausreichend Gewähr dafür bietet, dass er die für eine datenschutzgerechte Datenverarbeitung erforderlichen technischen und organisatorischen Maßnahmen zu treffen in der Lage ist. Der Auftrag ist schriftlich zu erteilen. Dabei sind insbesondere Gegenstand und Umfang der Datenverarbeitung, die notwendigen technischen und organisatorischen Maßnahmen, etwaige Unterauftragsverhältnisse sowie die Befugnis des Auftraggebers festzulegen, dass er hinsichtlich der Verarbeitung personenbezogener Daten dem Auftragnehmer Weisungen erteilen darf. Der Auftrag kann auch durch die Fachaufsichtsbehörde mit Wirkung für ihrer Aufsicht unterliegende Stellen des Landes erteilt werden; diese sind von der Auftragserteilung zu unterrichten. Der Auftraggeber hat sich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen durch den Auftragnehmer zu überzeugen.

(3) Ist der Auftragnehmer eine öffentliche Stelle, gelten für ihn nur die §§ 6, 9, 10, 27 bis 31, 40 und 41. Die Verarbeitung personenbezogener Daten ist nur im Rahmen des Auftrags und der Weisungen zulässig. Ist der Auftragnehmer der Ansicht, dass der Auftrag, einzelne Bestimmungen des Auftrags oder eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstoßen, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Soweit juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen dem Land oder der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, für eine öffentliche Stelle Daten im Auftrag verarbeiten, gelten die §§ 27 bis 31 entsprechend. Dies gilt nicht, soweit diese Personen oder Personenvereinigungen personenbezogene Daten im Auftrag eines der in § 2 Abs. 4 Satz 1 genannten Unternehmen oder deren Vereinigungen verarbeiten.

(5) Werden Wartungsarbeiten und vergleichbare Hilfstätigkeiten bei der Datenverarbeitung durch Stellen oder Personen außerhalb der verantwortlichen Stelle erbracht, gilt dies als Datenverarbeitung im Auftrag.

§ 8 Automatisiertes Abrufverfahren

(1) Ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, darf nur eingerichtet werden, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.

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

1. Anlass und Zweck des Abrufverfahrens,
2. Dritte, an die übermittelt wird,
3. Art der abzurufenden Daten,
4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

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

(3) Die Zulässigkeit des einzelnen Abrufs beurteilt sich nach den für die Erhebung und Übermittlung geltenden Vorschriften. Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit des Abrufs nur, wenn dazu Anlass be-

steht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

(4) Für die Einrichtung oder wesentliche Änderung eines automatisierten Verfahrens, das den Abruf personenbezogener Daten nur innerhalb einer öffentlichen Stelle ermöglicht, gelten die Absätze 1 und 2 entsprechend, wenn die Daten für einen anderen Zweck als den, für den sie gespeichert worden sind, genutzt werden sollen; dabei ist eine angemessene Abrufkontrolle zu gewährleisten.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

§ 8a Gemeinsame Verfahren

(1) Gemeinsame Verfahren sind automatisierte Verfahren, die mehreren verantwortlichen Stellen im Sinne dieses Gesetzes die Verarbeitung personenbezogener Daten in oder aus einem Datenbestand ermöglichen. Stellen, auf die dieses Gesetz keine Anwendung findet, können am gemeinsamen Verfahren beteiligt werden. Im Rahmen eines gemeinsamen Verfahrens obliegt die datenschutzrechtliche Verantwortung für die gespeicherten Daten jeweils den verantwortlichen Stellen, welche die Daten eingegeben haben. Soweit gemeinsame Verfahren Übermittlungen personenbezogener Daten durch Abruf ermöglichen, ist § 8 entsprechend anzuwenden. Auch die Abrufe personenbezogener Daten durch die am gemeinsamen Verfahren beteiligten Stellen sind zu protokollieren.

(2) Die Beteiligung öffentlicher Stellen des Landes nach § 2 Absatz 1 an gemeinsamen Verfahren ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit der Verarbeitung der Daten im Einzelfall bleiben unberührt.

(3) Vor der Einrichtung oder wesentlichen Änderung eines gemeinsamen Verfahrens ist eine Vorabkontrolle nach § 12 durchzuführen und die oder der Landesbeauftragte für den Datenschutz zu hören. Ihr oder ihm sind die Festlegungen nach Absatz 4, das Ergebnis der Vorabkontrolle sowie die Entwürfe der Regelungen nach Absatz 5 vorzulegen.

(4) Vor der Einrichtung oder wesentlichen Änderung eines gemeinsamen Verfahrens ist über die Angaben nach § 11 Absatz 2 hinaus schriftlich insbesondere festzulegen,

1. welche Verfahrensweise angewendet wird und welche der beteiligten Stellen jeweils für die Festlegung, Änderung, Fortentwicklung und Einhaltung von fachlichen und technischen Vorgaben für das gemeinsame Verfahren verantwortlich ist und
2. welche der beteiligten Stellen jeweils für die Rechtmäßigkeit der Datenverarbeitung welcher Daten verantwortlich ist.

Die nach Satz 1 Nummer 1 verantwortlichen Stellen bestimmen eine der beteiligten Stellen, die eine Kopie der von den beteiligten Stellen zu erstellenden Übersicht nach § 11 Absatz 2 verwahrt und diese nach § 11 Absatz 4 Satz 1 zusammen mit den Angaben nach Satz 1 Nummer 1 und 2 zur Einsichtnahme durch jedermann bereithält. Hat die nach Satz 2 bestimmte Stelle eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellt, ist diese oder dieser für die Verwahrung und die Einsichtnahme durch jedermann zuständig. Nach Satz 1 Nummer 1 können auch verantwortliche Stellen bestimmt werden, die andere Stellen mit der Verarbeitung personenbezogener Daten für das gemeinsame Verfahren beauftragen dürfen. § 7 bleibt unberührt.

(5) Soweit für die beteiligten Stellen unterschiedliche Datenschutzvorschriften gelten, können die beteiligten Stellen das gemeinsame Verfahren erst einrichten und nutzen, wenn vor Einrichtung eines gemeinsamen Verfahrens geregelt ist, welches Datenschutzrecht angewendet wird und welche Kontrollstellen die Einhaltung der Datenschutzvorschriften prüfen.

(6) Die Betroffenen können ihre Rechte nach den §§ 21 bis 24 gegenüber jeder der beteiligten Stellen geltend machen, unabhängig davon, welche Stelle im Einzelfall für die Verarbeitung der jeweiligen Daten nach Absatz 4 Satz 1 Nummer 2 verantwortlich ist. Die Stelle, an die sich die Betroffenen wenden,

leitet das Anliegen an die jeweils zuständige Stelle weiter. Die Betroffenen sind über die Weiterleitung zu unterrichten.

§ 9

Technische und organisatorische Maßnahmen

(1) Die Gestaltung und Auswahl der technischen Einrichtungen und der Verfahren zur automatisierten Verarbeitung personenbezogener Daten hat sich an dem Grundsatz auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu verarbeiten.

(2) Öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Datenverarbeitung zu gewährleisten. Erforderlich sind Maßnahmen, wenn ihr Aufwand, insbesondere unter Berücksichtigung der Art der zu schützenden personenbezogenen Daten, in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

(3) Werden personenbezogene Daten automatisiert verarbeitet, sind je nach Art und Verwendung der zu schützenden personenbezogenen Daten und unter Berücksichtigung des Standes der Technik Maßnahmen zu treffen, die geeignet sind,

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

(4) Die Landesregierung wird ermächtigt, die in Absatz 3 genannten Anforderungen nach dem jeweiligen Stand der Technik und Organisation durch Rechtsverordnung fortzuschreiben.

(5) Werden personenbezogene Daten in nicht automatisierten Dateien oder in Akten verarbeitet, sind insbesondere Maßnahmen zu treffen, um zu verhindern, dass Unbefugte bei der Bearbeitung, der Aufbewahrung, dem Transport und der Vernichtung auf die Daten zugreifen können.

§ 10 Behördlicher Datenschutzbeauftragter

(1) Öffentliche Stellen können einen behördlichen Datenschutzbeauftragten bestellen. Die Bestellung bedarf der Schriftform.

(2) Bestellt werden darf nur, wer die zur Erfüllung seiner Aufgaben erforderliche Sachkunde und Zuverlässigkeit besitzt und durch die Bestellung keinem Interessenkonflikt ausgesetzt wird. Die öffentliche Stelle kann einen Bediensteten ihrer Aufsichtsbehörde mit deren Zustimmung zum Beauftragten für den Datenschutz bestellen. Mehrere Stellen können gemeinsam einen Datenschutzbeauftragten bestellen.

(3) Der behördliche Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben der Behördenleitung unmittelbar zu unterstellen. Er ist bei der Erfüllung seiner Aufgaben weisungsfrei und darf deswegen nicht benachteiligt werden.

(4) Der behördliche Datenschutzbeauftragte hat die Aufgabe, die öffentliche Stelle bei der Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz zu unterstützen. Zu seinen Aufgaben gehört es insbesondere,

1. auf die Einhaltung der Datenschutzvorschriften bei der Planung, Einführung und Anwendung von Verfahren, mit denen personenbezogene Daten automatisiert verarbeitet werden, hinzuwirken,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz und den besonderen Erfordernissen des Datenschutzes in ihrem Tätigkeitsbereich vertraut zu machen sowie
3. das Verzeichnisse (§ 11) zu führen.

Der behördliche Datenschutzbeauftragte ist vor dem Einsatz oder der wesentlichen Änderung eines automatisierten Verfahrens rechtzeitig zu unterrichten.

§ 11 Verfahrensverzeichnis

(1) Jede öffentliche Stelle führt ein Verzeichnis der automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden (Verfahrensverzeichnis). Das Verzeichnis kann auch von einer Stelle für andere Stellen geführt werden.

(2) In das Verzeichnis sind einzutragen:

1. Name und Anschrift der verantwortlichen Stelle,
2. die Bezeichnung des Verfahrens,
3. die Zweckbestimmung und die Rechtsgrundlage der Verarbeitung,
4. die Art der gespeicherten Daten,
5. der Kreis der Betroffenen,
6. die Empfänger der Daten oder Gruppen von Empfängern sowie die jeweiligen Datenarten, wenn vorgesehen ist,
 - a) die Daten zu übermitteln,

- b) sie innerhalb der öffentlichen Stelle für einen weiteren Zweck zu nutzen oder
 - c) sie im Auftrag verarbeiten zu lassen,
7. die Fristen für die Prüfung der Sperrung und Löschung der Daten oder für die Sperrung und Löschung,
 8. die zugriffsberechtigten Personengruppen oder Personen, die allein zugriffsberechtigt sind,
 9. eine allgemeine Beschreibung der eingesetzten Hardware, der Vernetzung und der Software und
 10. die technischen und organisatorischen Maßnahmen nach § 9.

(3) Absatz 1 gilt nicht für Verfahren, deren einziger Zweck das Führen eines Registers ist, das zur Information der Öffentlichkeit bestimmt ist und allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, sowie für Verfahren, die allgemeinen Verwaltungszwecken dienen, insbesondere Verfahren der Textverarbeitung.

(4) Die öffentliche Stelle macht die Angaben nach Absatz 2 Nr. 1 bis 7 des Verfahrensverzeichnis auf Antrag jedermann in geeigneter Weise verfügbar. Satz 1 findet keine Anwendung auf Verfahren des Landesamts für Verfassungsschutz.

§ 12 Vorabkontrolle

Wer für den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten zuständig ist, das mit besonderen Gefahren für das Persönlichkeitsrecht verbunden sein kann, insbesondere auf Grund der Art oder der Zweckbestimmung der Verarbeitung, darf das Verfahren erst einsetzen, wenn sichergestellt ist, dass diese Gefahren nicht bestehen oder durch technische oder organisatorische Maßnahmen verhindert werden; dies gilt insbesondere für die Einrichtung eines automatisierten Abrufverfahrens nach § 8, für automatisierte Verfahren, mit denen Daten nach § 33 verarbeitet werden, und für die Herausgabe von Datenträgern nach § 5 Abs. 2. Das Ergebnis der Untersuchung und dessen Begründung sind aufzuzeichnen und dem behördlichen Datenschutzbeauftragten oder, wenn ein solcher nicht bestellt ist, dem Landesbeauftragten für den Datenschutz zur Prüfung zuzuleiten. Der behördliche Datenschutzbeauftragte wendet sich in Zweifelsfällen an den Landesbeauftragten für den Datenschutz.

ZWEITER ABSCHNITT

Rechtsgrundlagen der Datenverarbeitung

§ 13 Erhebung

- (1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der erhebenden Stelle erforderlich ist.
- (2) Personenbezogene Daten, die nicht aus allgemein zugänglichen Quellen entnommen werden, sind beim Betroffenen mit seiner Kenntnis zu erheben.
- (3) Personenbezogene Daten dürfen beim Betroffenen ohne seine Kenntnis nur erhoben werden, wenn
 1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
 2. die zu erfüllende Aufgabe ihrer Art nach eine solche Erhebung erforderlich macht und keine Anhaltspunkte dafür vorliegen, dass ihr überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Bei Dritten dürfen personenbezogene Daten nur erhoben werden, wenn

1. einer der in § 15 Abs. 2 Nr. 1 bis 6 genannten Fälle vorliegt oder
2. die zu erfüllende Aufgabe ihrer Art nach eine solche Erhebung erforderlich macht und keine Anhaltspunkte dafür vorliegen, dass ihr überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

§ 14

Unterrichtung bei der Erhebung

(1) Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben, sind ihm gegenüber anzugeben:

1. die beabsichtigte Datenverarbeitung und der Zweck der Verarbeitung sowie
2. bei einer beabsichtigten Übermittlung auch die Empfänger der Daten oder Gruppen von Empfängern, soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss.

Werden die Daten auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechten, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Über die der Auskunftspflicht zugrunde liegende Rechtsvorschrift und die Folgen der Verweigerung von Angaben ist der Betroffene bei Verwendung eines Erhebungsvordrucks stets, sonst nur auf Verlangen aufzuklären. Bei Verwendung eines Erhebungsvordrucks ist der Betroffene auch auf das Bestehen von Auskunfts- und Berichtigungsrechten hinzuweisen.

(2) Werden Daten beim Betroffenen ohne seine Kenntnis oder bei Dritten erhoben, ist der Betroffene entsprechend Absatz 1 Satz 1 zu benachrichtigen, wenn die Daten in einer Datei gespeichert werden. Bei schriftlicher Benachrichtigung ist der Betroffene auch auf das Bestehen von Auskunfts- und Berichtigungsrechten hinzuweisen. Die Benachrichtigung erfolgt zum Zeitpunkt der Speicherung oder im Fall einer beabsichtigten Übermittlung spätestens bei der ersten Übermittlung. Sätze 1 bis 3 finden keine Anwendung auf Verfahren des Landesamts für Verfassungsschutz.

(3) Eine Pflicht zur Benachrichtigung besteht in den Fällen des Absatzes 2 nicht, wenn

1. die Verarbeitung der Daten durch Gesetz ausdrücklich vorgesehen ist,
2. der Betroffene auf andere Weise Kenntnis von der Verarbeitung seiner Daten erlangt,
3. die Benachrichtigung des Betroffenen einen unverhältnismäßigen Aufwand erfordern würde,
4. die Benachrichtigung die ordnungsgemäße Erfüllung von Aufgaben der Gefahrenabwehr oder von Aufgaben der Finanzverwaltung im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung oder die Verfolgung von Straftaten oder Ordnungswidrigkeiten gefährden würde,
5. die Benachrichtigung die Sicherheit des Bundes oder eines Landes gefährden würde,
6. die Daten oder die Tatsache ihrer Speicherung zum Schutze des Betroffenen oder zum Schutze der Rechte Dritter geheim gehalten werden müssen und deshalb das Interesse des Betroffenen an der Benachrichtigung zurücktreten muss oder
7. die Daten ausschließlich für Zwecke der wissenschaftlichen Forschung oder der Statistik verarbeitet werden.

(4) Werden personenbezogene Daten bei einem Dritten außerhalb des öffentlichen Bereichs erhoben, so ist er auf Verlangen auf den Erhebungszweck hinzuweisen, soweit dadurch schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden. Werden die Daten auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, so ist er auf die Auskunftspflicht, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Über die der Auskunftspflicht zugrunde liegende Rechtsvorschrift und die Folgen der Verweigerung von Angaben ist er bei Verwendung eines Erhebungsvordrucks stets, sonst nur auf Verlangen aufzuklären.

§ 15 Speicherung, Veränderung und Nutzung

(1) Das Speichern, Verändern und Nutzen personenbezogener Daten ist zulässig, wenn es

1. zur Erfüllung der Aufgaben der öffentlichen Stelle erforderlich ist und
2. für Zwecke erfolgt, für die die Daten erhoben worden sind; ist keine Erhebung vorausgegangen, dürfen die Daten nur für Zwecke genutzt werden, für die sie erstmals gespeichert worden sind.

(2) Das Speichern, Verändern und Nutzen personenbezogener Daten für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,
2. der Betroffene eingewilligt hat oder offensichtlich ist, dass dies im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er seine Einwilligung hierzu verweigern würde,
3. der Betroffene einer durch Rechtsvorschrift festgelegten Auskunftspflicht nicht nachgekommen und über die beabsichtigte Datenverarbeitung unterrichtet worden ist,
4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
5. 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,
6. die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, es sei denn, dass überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen,
7. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen, oder
8. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist.

(3) Eine Speicherung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung, der Durchführung von Organisationsuntersuchungen, der Prüfung und Wartung von automatisierten Verfahren der Datenverarbeitung sowie statistischen Zwecken oder Zwecken der Durchführung eigener wissenschaftlicher Forschung der speichernden Stelle dient. Dies gilt auch für die Speicherung und Nutzung zu Ausbildungs- und Prüfungszwecken, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diesen Zweck und hiermit in Zusammenhang stehenden Maßnahmen gegenüber Bediensteten genutzt werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 bis 3 gespeichert werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten in Akten so verbunden, dass eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so ist die Speicherung auch dieser Daten zulässig, soweit nicht schutzwürdige Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen. Unter denselben Voraussetzungen dürfen die für die Aufgabenerfüllung nicht erforderlichen Daten innerhalb der speichernden Stelle weitergegeben werden; eine darüber hinausgehende Nutzung dieser Daten ist unzulässig.

§ 16 Übermittlung an Stellen innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Stellen innerhalb des öffentlichen Bereichs ist zulässig, wenn sie

1. zur Erfüllung der Aufgaben der übermittelnden Stelle oder der Stelle, an die die Daten übermittelt werden, erforderlich ist und
2. für Zwecke erfolgt, für die eine Nutzung nach § 15 Abs. 1 bis 4 zulässig wäre.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen einer öffentlichen Stelle im Geltungsbereich des Grundgesetzes, trägt diese die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 8 Abs. 3 Satz 2 und 3 bleibt unberührt.

(3) Die Stelle, an die die Daten übermittelt werden, darf sie nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihr übermittelt worden sind. Eine Verarbeitung für andere Zwecke ist nur unter den Voraussetzungen des § 15 Abs. 2 zulässig.

(4) Auf die Übermittlung verbundener Daten findet § 15 Abs. 5 entsprechende Anwendung.

§ 17 Übermittlung an Stellen der öffentlich-rechtlichen Religionsgesellschaften

Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gilt § 16 Abs. 1 bis 3 entsprechend, sofern für diese Stellen ausreichende Datenschutzregelungen gelten. Die Feststellung hierüber trifft das Innenministerium.

§ 18 Übermittlung an Stellen außerhalb des öffentlichen Bereichs

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

1. sie zur Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist und für Zwecke erfolgt, für die eine Nutzung nach § 15 Abs. 1 bis 4 zulässig wäre, oder
2. der Dritte, an den die Daten übermittelt werden sollen, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse am Ausschluss der Übermittlung hat.

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

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten, insbesondere über den Dritten, an den die Daten übermittelt werden, und den Zweck der Übermittlung. Dies gilt nicht, wenn die Unterrichtung einen unverhältnismäßigen Aufwand erfordern würde, der Betroffene von der Übermittlung auf andere Weise Kenntnis erlangt, die Unterrichtung wegen der Art der personenbezogenen Daten unter Berücksichtigung der schutzwürdigen Interessen des Betroffenen nicht geboten erscheint oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Die Stelle, an die die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihr übermittelt worden sind. Die übermittelnde Stelle hat sie in den Fällen des Absatzes 1 Nr. 2 hierauf hinzuweisen. Eine Verarbeitung für andere Zwecke ist nur zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle eingewilligt hat.

(5) Die übermittelnde Stelle soll die Übermittlung mit Auflagen versehen, die den Datenschutz bei dem Dritten, an den die Daten übermittelt werden, sicherstellen, oder mit dem Dritten Vereinbarungen zur Gewährleistung des Datenschutzes treffen.

§ 19 Übermittlung für Zwecke der wissenschaftlichen Forschung

(1) Die Übermittlung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung an Stellen innerhalb des öffentlichen Bereichs ist zulässig, wenn dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen am Ausschluss der Übermittlung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Kann der Zweck der Forschung auch mit anonymisierten Daten erreicht werden und steht der verantwortlichen Stelle nicht ausreichend Personal für eine Anonymisierung der Daten zur Verfügung, können die mit der Durchführung des Forschungsvorhabens befassten Personen diese Aufgabe für die verantwortliche Stelle unter deren Aufsicht wahrnehmen. Die betreffenden Personen sind zuvor nach dem Verpflchtungsgesetz zu verpflichten.

(2) Für die Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs gilt Absatz 1 mit der Maßgabe, dass die Übermittlung nur zulässig ist, wenn sich die Stelle verpflichtet, die übermittelten Daten nicht für andere Zwecke zu verarbeiten und die Bestimmungen des § 35 Abs. 2 und 3 einzuhalten.

§ 20 Übermittlung an Stellen außerhalb des Geltungsbereichs des Grundgesetzes

(1) Für die Übermittlung personenbezogener Daten an Stellen

1. in anderen Mitgliedstaaten der Europäischen Union,
2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder
3. der Organe und Einrichtungen der Europäischen Gemeinschaften
gelten §§ 16, 18 und 19 entsprechend.

(2) Die Übermittlung personenbezogener Daten in Staaten außerhalb der Europäischen Union oder an über- oder zwischenstaatliche Stellen ist unter den Voraussetzungen der §§ 18 und 19 zulässig, soweit in den folgenden Absätzen nichts anderes bestimmt ist.

(3) Die Übermittlung unterbleibt, soweit

1. Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde, oder
2. der Betroffene ein überwiegendes schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn in dem Staat außerhalb der Europäischen Union oder bei der über- oder zwischenstaatlichen Stelle ein angemessenes Datenschutzniveau nicht gewährleistet ist.

Die Angemessenheit des Datenschutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den Empfänger geltenden Rechtsnormen sowie die dort geltenden Landesregeln und Sicherheitsmaßnahmen herangezogen werden.

(4) Ist in dem Staat, in den die Daten übermittelt werden sollen, kein angemessenes Datenschutzniveau gewährleistet, ist die Übermittlung nur zulässig, wenn

1. der Betroffene eingewilligt hat,
2. die Übermittlung für die Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung rechtlicher Ansprüche vor Gericht einschließlich eines Vorverfahrens erforderlich ist,
3. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder
4. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

(5) Ist in dem Staat, in den die Daten übermittelt werden sollen, kein angemessenes Datenschutzniveau gewährleistet, ist unbeschadet des Absatzes 4 eine Übermittlung auch zulässig, wenn die Person oder Stelle, an die die Daten übermittelt werden sollen, ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; diese Garantien können sich auch aus Vertragsklauseln ergeben.

§ 20a Videobeobachtung und Videoaufzeichnung (Videoüberwachung)

(1) Mit Hilfe optisch-elektronischer Einrichtungen dürfen personenbezogene Daten erhoben werden (Videobeobachtung), wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist,

1. um Leben, Gesundheit, Freiheit oder Eigentum von Personen, die sich in öffentlichen Einrichtungen, öffentlichen Verkehrsmitteln, Amtsgebäuden oder sonstigen baulichen Anlagen öffentlicher Stellen oder in deren unmittelbarer Nähe aufhalten, oder
2. um Kulturgüter, öffentliche Einrichtungen, öffentliche Verkehrsmittel, Amtsgebäude oder sonstige bauliche Anlagen öffentlicher Stellen sowie die dort oder in deren unmittelbarer Nähe befindlichen Sachen

zu schützen, insbesondere die Begehung von Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten zu verhindern oder deren Verfolgung oder die Geltendmachung von Rechtsansprüchen zu ermöglichen. Die Videobeobachtung ist nur zulässig, wenn

1. Tatsachen die Annahme rechtfertigen, dass die in Satz 1 genannten Rechtsgüter, Einrichtungen oder Objekte gefährdet sind und

2. keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Die Videobeobachtung und die erhebende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Speicherung (Videoaufzeichnung), Übermittlung und Nutzung der nach Absatz 1 erhobenen Daten ist zulässig, soweit sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden. Für einen anderen Zweck dürfen die Daten nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über die Tatsache der Speicherung zu benachrichtigen. § 14 Abs. 2 und 3 findet entsprechende Anwendung.

(5) Die Videoaufzeichnungen und daraus gefertigte oder sich auf die Videoüberwachung beziehende Unterlagen sind unverzüglich, spätestens jedoch vier Wochen nach der Datenerhebung zu löschen, soweit sie nicht zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.

(6) Der erstmalige Einsatz optisch-elektronischer Einrichtungen bedarf der vorherigen schriftlichen Freigabe durch die verantwortliche Stelle. Die schriftliche Freigabe hat folgende Angaben und Begründungen zu enthalten:

1. Zweck der Videoüberwachung,
2. Darlegung der Erforderlichkeit der Videobeobachtung und gegebenenfalls der Videoaufzeichnung, insbesondere auch in Bezug auf die räumliche Ausdehnung und den zeitlichen Umfang,
3. Tatsachen im Sinne des Absatzes 1 Satz 2 Nr. 1,
4. eine Abwägung mit den Interessen der Betroffenen,
5. Maßnahmen nach Absatz 2,
6. Namen der zugriffsberechtigten Personen und vorgesehene Datennutzungen und -übermittlungen,
7. Zeitpunkt der Löschung und gegebenenfalls Fristen für die Prüfung der Löschung sowie die hierfür maßgeblichen Erwägungen und
8. technische und organisatorische Maßnahmen nach § 9.

Ist ein behördlicher Datenschutzbeauftragter bestellt, ist diesem der Entwurf der schriftlichen Freigabe zur Prüfung zuzuleiten. Für Änderungen des Verfahrens gelten die Sätze 1 bis 3 entsprechend.

DRITTER ABSCHNITT

Rechte des Betroffenen

§ 21 Auskunft

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

1. die zu seiner Person gespeicherten Daten,

2. den Zweck der Verarbeitung,
3. die Herkunft der Daten, soweit diese gespeichert oder sonst bekannt ist, und die Empfänger oder Gruppen von Empfängern, an die die Daten übermittelt werden sollen, sowie
4. den strukturierten Ablauf der automatisierten Verarbeitung der ihn betreffenden Daten in den Fällen des § 4 Abs. 7 und die dabei herangezogenen Entscheidungskriterien.

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

(2) In dem Antrag soll die Art der personenbezogenen Daten näher bezeichnet werden, über die Auskunft erteilt werden soll. Sind die personenbezogenen Daten in Akten gespeichert, wird Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht.

(3) Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen. Sind die Daten in Akten gespeichert, ist dem Betroffenen auf Verlangen Akteneinsicht zu gewähren; Absatz 2 Satz 2 findet entsprechende Anwendung. Ein Recht auf Akteneinsicht besteht nicht, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft zu erteilen. Rechtsvorschriften über die Akteneinsicht im Verwaltungsverfahren bleiben unberührt.

(4) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Behörden der Staatsanwaltschaften, an Polizeidienststellen, Verfassungsschutzbehörden und Behörden der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, ist sie nur mit Zustimmung dieser oder der nach Absatz 7 zuständigen Stelle zulässig. Satz 1 findet auch Anwendung auf die Übermittlung personenbezogener Daten an den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung. Für die Versagung der Zustimmung gelten die Absätze 5 und 6 entsprechend.

(5) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen überwiegender berechtigter Interessen eines Dritten, geheim gehalten werden müssen

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

(6) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er den Landesbeauftragten für den Datenschutz anrufen kann.

(7) Die fachlich zuständige oberste Landesbehörde kann durch Rechtsverordnung bestimmen, dass eine andere als die speichernde Stelle die Auskunft erteilt.

§ 22 Berichtigung

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

(2) Von der Berichtigung unrichtiger Daten sind die Empfänger der Daten zu verständigen, soweit dies zur Wahrung schutzwürdiger Interessen des Betroffenen oder zur Erfüllung der Aufgaben der verantwortlichen Stelle oder des Empfängers erforderlich erscheint; dies gilt nicht, wenn dies einen unverhältnismäßigen Aufwand erfordern würde.

§ 23 Löschung

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

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

(2) Personenbezogene Daten in Akten sind zu löschen, wenn die speichernde Stelle im Einzelfall feststellt, dass die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist.

(3) Vor einer Löschung sind die Daten dem zuständigen Archiv nach Maßgabe der §§ 3, 7 und 8 des Landesarchivgesetzes zur Übernahme anzubieten.

(4) Die Löschung unterbleibt, wenn

1. Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder
2. sie wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(5) Von einer Löschung unzulässig gespeicherter Daten sind die Empfänger der Daten nach Maßgabe des § 22 Abs. 2 zu verständigen.

§ 24 Sperrung

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

1. ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt oder
2. in den Fällen des § 23 Abs. 4 eine Löschung unterbleibt.

(2) Personenbezogene Daten in Akten sind zu sperren, wenn die speichernde Stelle im Einzelfall feststellt, dass die Daten unzulässig gespeichert sind. Sie sind ferner zu sperren, wenn die speichernde Stelle im Einzelfall feststellt, dass die Daten zur Aufgabenerfüllung nicht mehr erforderlich sind, eine Löschung nach § 23 Abs. 2 nicht in Betracht kommt und ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden.

(3) Gesperrte personenbezogene Daten sind gesondert aufzubewahren; bei automatisierten Verfahren kann die Sperrung stattdessen auch durch zusätzliche technische Maßnahmen gewährleistet werden. Lassen sich auf Grund der Art der Verarbeitung Maßnahmen nach Satz 1 nicht oder nur mit unverhältnismäßig hohem Aufwand durchführen, sind die Daten mit einem Sperrvermerk zu versehen.

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

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

Personenbezogene Daten, die unzulässig in Akten gespeichert sind, dürfen ohne Einwilligung des Betroffenen nicht mehr genutzt oder übermittelt werden.

(5) Von einer Sperrung unzulässig gespeicherter Daten sind die Empfänger der Daten nach Maßgabe des § 22 Abs. 2 zu verständigen.

§ 25 Schadensersatz

(1) Fügt eine öffentliche Stelle dem Betroffenen durch eine nach den Vorschriften dieses Gesetzes oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Verarbeitung seiner personenbezogenen Daten in oder aus Dateien einen Schaden zu, ist sie dem Betroffenen zum Ersatz des daraus entstehenden Schadens verpflichtet. Dies gilt nicht, wenn die öffentliche Stelle nachweist, dass der Umstand, durch den der Schaden eingetreten ist, nicht von ihr zu vertreten ist.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt bis zu einem Betrag in Höhe von 130 000 Euro begrenzt. Ist auf Grund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130 000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

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

(5) Mehrere Ersatzpflichtige haften als Gesamtschuldner.

(6) Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, so gilt § 254 des Bürgerlichen Gesetzbuches entsprechend. Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

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

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

VIERTER ABSCHNITT

Landesbeauftragter für den Datenschutz

§ 26 Bestellung und Rechtsstellung

(1) ^{*)} Auf Vorschlag der Landesregierung wählt der Landtag mit der Mehrheit seiner Mitglieder einen Landesbeauftragten für den Datenschutz. Dieser muss die Befähigung zum Richteramt oder zum höheren Verwaltungsdienst haben oder für eine andere Laufbahn des höheren Dienstes befähigt sein. Der Landesbeauftragte für den Datenschutz wird jeweils für die Dauer von sechs Jahren in ein Beamtenverhältnis auf Zeit berufen. Einmalige Wiederwahl ist zulässig.

(2) Der Landesbeauftragte für den Datenschutz ist in Ausübung seines Amtes völlig unabhängig und nur dem Gesetz unterworfen. Er unterliegt keiner Rechts- und Fachaufsicht.

(3) Die Dienststelle des Landesbeauftragten für den Datenschutz wird beim Landtag eingerichtet. Der Landesbeauftragte für den Datenschutz trifft die Entscheidungen nach § 37 des Beamtenstatusgesetzes für sich und seine Mitarbeiter in eigener Verantwortung. Er untersteht der Dienstaufsicht des Präsidenten des Landtags nur insoweit, als seine völlige Unabhängigkeit dadurch nicht beeinträchtigt wird. Die für Richter auf Lebenszeit geltenden Vorschriften über die Dienstaufsicht, die Teilzeitbeschäftigung, Urlaub von längerer Dauer ohne Dienstbezüge, die Altersteilzeit, die Altersgrenze, die Abordnung, die Versetzung in ein anderes Amt, die Versetzung in den Ruhestand, die eingeschränkte Verwendung wegen begrenzter Dienstfähigkeit, die Entlassung, die Amtsenthebung, die vorläufige Untersagung der Amtsgeschäfte und über Disziplinarmaßnahmen sind auf den Landesbeauftragten für den Datenschutz sinngemäß anzuwenden. Im Falle des Satzes 4 sind die Vorschriften des Landesrichtergesetzes und des Deutschen Richtergesetzes über Disziplinarverfahren, Versetzungs- und Prüfungsverfahren und Richterdienstgerichte sinngemäß und mit der Maßgabe anzuwenden, dass bei den Dienstgerichten nur Richter aus der Verwaltungsgerichtsbarkeit mitwirken. Das Dienstgericht entscheidet in der Besetzung mit einem Vorsitzenden und zwei Beisitzern, der Dienstgerichtshof in der Besetzung mit einem Vorsitzenden und vier Beisitzern. Für das Dienstgericht bestimmt das Präsidium des Landgerichts Karlsruhe und für den Dienstgerichtshof das Präsidium des Oberlandesgerichts Stuttgart die Vorsitzenden, die Beisitzer und deren Vertreter aus den Vorschlagslisten der Verwaltungsgerichtsbarkeit. Das Antragsrecht zur Einleitung eines förmlichen Disziplinarverfahrens und für ein Vorermittlungsverfahren übt hinsichtlich des Landesbeauftragten für den Datenschutz der Präsident des Landtags aus.

(4) Dem Landesbeauftragten für den Datenschutz ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen. Die Besetzung der Personalstellen erfolgt im Einvernehmen mit dem Landesbeauftragten für den Datenschutz. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt, abgeordnet oder umgesetzt werden. Ihre Einbeziehung in den allgemeinen Personalaustausch der Landesverwaltung wird von der Landesregierung gewährleistet.

(5) Ist der Landesbeauftragte für den Datenschutz an der Ausübung seines Amtes verhindert, nimmt der leitende Beamte der Dienststelle des Landesbeauftragten für den Datenschutz dessen Geschäfte wahr. Geht die Dauer der Verhinderung über drei Monate hinaus, kann der Präsident des Landtags einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen; der Landesbeauftragte für den Datenschutz soll dazu gehört werden.

Fußnoten

- * [Gemäß Artikel 8 Abs. 4 des Gesetzes vom 7. Februar 2011 (GBl. S. 43, 46) gilt abweichend von Artikel 1 Nr. 4 Buchst. a § 26 Abs. 1 für die Bestellung und die Amtszeit des zum Zeitpunkt des Inkrafttretens dieses Gesetzes amtierenden Landesbeauftragten für den Datenschutz während der laufenden Amtszeit § 26 Abs. 1 des Landesdatenschutzgesetzes in der bisher geltenden Fassung fort.]

§ 27

Anrufung des Landesbeauftragten für den Datenschutz

(1) Jeder kann sich an den Landesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch eine öffentliche Stelle in seinen Rechten verletzt worden zu sein. Niemand darf benachteiligt oder gemaßregelt werden, weil er von seinem Recht nach Satz 1 Gebrauch gemacht hat.

(2) Wendet sich ein Betroffener an den Landesbeauftragten für den Datenschutz, weil ihm nach § 21 Abs. 5 oder besonderen gesetzlichen Vorschriften keine Auskunft erteilt worden ist, darf die Mitteilung des Landesbeauftragten für den Datenschutz an den Betroffenen keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese oder die nach § 21 Abs. 7 zuständige Stelle nicht einer weitergehenden Auskunft zustimmt. Das Gleiche gilt, wenn ein Betroffener unmittelbar den Landesbeauftragten für den Datenschutz anruft und die für die Erteilung der Auskunft zuständige Stelle

le diesem unter Angabe von Gründen darlegt, dass sie bei einem Auskunftsersuchen eine Auskunft nach den in Satz 1 genannten Vorschriften verweigern würde.

§ 28 Kontrolle durch den Landesbeauftragten für den Datenschutz

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

(2) Die Kontrolle des Landesbeauftragten für den Datenschutz erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen. Für personenbezogene Daten in Dateien oder Akten über die Sicherheitsüberprüfung gilt dies jedoch nur, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten nicht widersprochen hat. Die speichernde Stelle hat die Betroffenen im Einzelfall oder in allgemeiner Form auf das Widerspruchsrecht hinzuweisen. Der Widerspruch ist schriftlich gegenüber der speichernden Stelle oder dem Landesbeauftragten für den Datenschutz zu erklären.

(3) Die Kontrolle des Landesbeauftragten für den Datenschutz erstreckt sich nicht auf personenbezogene Daten, die der Kontrolle durch die Kommission nach § 2 des Ausführungsgesetzes zum Artikel 10-Gesetz unterliegen, es sei denn, die Kommission ersucht den Landesbeauftragten für den Datenschutz, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten.

(4) Stellt der Landesbeauftragte für den Datenschutz bei seiner Kontrolle einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist er befugt, diesen bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen.

§ 29 Pflicht zur Unterstützung

(1) Die öffentlichen Stellen sind verpflichtet, den Landesbeauftragten für den Datenschutz und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist im Rahmen der Kontrollbefugnis nach § 28 insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten, insbesondere in die gespeicherten Daten und die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,
2. jederzeit Zutritt zu den Diensträumen zu gewähren.

(2) Für die in § 21 Abs. 4 Satz 1 genannten öffentlichen Stellen besteht die Pflicht zur Unterstützung nur gegenüber dem Landesbeauftragten für den Datenschutz selbst und den von ihm oder dem leitenden Beamten seiner Dienststelle schriftlich besonders Beauftragten. Absatz 1 Satz 2 findet für diese Stellen keine Anwendung, soweit die jeweils zuständige oberste Landesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

§ 30 Mitteilung des Ergebnisses der Kontrolle, Beanstandungen

(1) Der Landesbeauftragte für den Datenschutz teilt der verantwortlichen Stelle das Ergebnis seiner Kontrolle mit. Damit können Vorschläge zur Verbesserung des Datenschutzes verbunden werden, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung personenbezogener Daten.

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

1. bei den öffentlichen Stellen des Landes gegenüber der zuständigen obersten Landesbehörde,

2. bei den Gemeinden, Gemeindeverbänden und den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts sowie bei den in § 2 Abs. 2 genannten Stellen gegenüber dem vertretungsberechtigten Organ

und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden angemessenen Frist auf. In den Fällen des Satzes 1 Nr. 2 unterrichtet der Landesbeauftragte für den Datenschutz gleichzeitig die zuständige Aufsichtsbehörde.

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

(4) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Landesbeauftragten für den Datenschutz getroffen worden oder beabsichtigt sind. Die in Absatz 2 Satz 1 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme an den Landesbeauftragten für den Datenschutz zu.

§ 31 **Weitere Aufgaben des Landesbeauftragten** **für den Datenschutz ^{*)} ^{**)}**

(1) Der Landesbeauftragte für den Datenschutz ist auch Aufsichtsbehörde nach dem Bundesdatenschutzgesetz für den Datenschutz im nichtöffentlichen Bereich.

(2) Der Landesbeauftragte für den Datenschutz erstattet dem Landtag zum 1. Dezember jedes zweiten Jahres einen Bericht über seine Tätigkeit im öffentlichen und im nichtöffentlichen Bereich. Dieser ist zu veröffentlichen.

(3) Der Landesbeauftragte für den Datenschutz hat auf Anforderung des Landtags Gutachten zu erstellen und besondere Berichte zu erstatten. Er hat ferner zu parlamentarischen Anfragen von Abgeordneten Stellung zu nehmen, die den Datenschutz in dem seiner Kontrolle unterliegenden Bereich betreffen. Er kann sich jederzeit an den Landtag wenden, damit ihn dieser bei der Wahrnehmung seiner Aufgaben unterstützt. Der Landesbeauftragte für den Datenschutz unterrichtet den Ständigen Ausschuss des Landtags halbjährlich, aus besonderem Anlass auch unverzüglich, über aktuelle Entwicklungen im Bereich des Datenschutzes und über datenschutzrechtliche Angelegenheiten von grundsätzlicher oder wesentlicher Bedeutung. Eine Unterrichtung erfolgt auch, wenn der Ständige Ausschuss des Landtags darum ersucht.

(4) Der Landesbeauftragte für den Datenschutz kann der Landesregierung und einzelnen Ministerien sowie anderen öffentlichen Stellen Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Er ist bei der Ausarbeitung von Rechts- und Verwaltungsvorschriften zu beteiligen, wenn sie die Verarbeitung personenbezogener Daten betreffen.

(5) Der Landesbeauftragte für den Datenschutz leistet den anderen Kontrollstellen in den Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe).

Fußnoten

* Artikel 1 Nr. 5 Buchst a [betrifft § 31 Absätze 1 bis 3] 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).

** Gemäß Artikel 8 Absatz 1 des Gesetzes vom 7. Februar 2011 (GBl. S. 43, 46) legt der Landesbeauftragte für den Datenschutz anstelle des zum 1. Juli 2011 fälligen Tätigkeitsberichts zum Datenschutz im nichtöffentlichen Bereich zum 1. Dezember 2011 den ersten gemeinsamen Tätigkeitsbericht nach Artikel 1 Nr. 5 Buchst. a [betrifft § 31 Absätze 1 bis 3] vor.

§ 32

Meldung an den Landesbeauftragten für den Datenschutz

(1) Die öffentlichen Stellen, die keinen Datenschutzbeauftragten nach § 10 bestellt haben, melden dem Landesbeauftragten für den Datenschutz den Einsatz und die wesentliche Veränderung eines automatisierten Verfahrens. Ausgenommen sind die in § 11 Abs. 3 und 4 Satz 2 genannten Verfahren.

(2) Die meldepflichtigen Stellen haben spätestens gleichzeitig mit der ersten Einspeicherung die Angaben nach § 11 Abs. 2 mitzuteilen.

§ 32a Gebühren für Amtshandlungen im nichtöffentlichen Bereich

Der Landesbeauftragte für den Datenschutz kann für individuell zurechenbare Amtshandlungen im nichtöffentlichen Bereich Gebühren und Auslagen festsetzen. Die Ausübung des Ermessens bedarf keiner Begründung. Das Innenministerium legt im Einvernehmen mit dem Landesbeauftragten für den Datenschutz durch Rechtsverordnung die Gebührentatbestände und die Höhe der Gebühren fest.

FÜNFTER ABSCHNITT

Besondere Bestimmungen

§ 33 Verarbeitung besonderer Arten personenbezogener Daten

(1) Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben hervorgehen, dürfen nur verarbeitet werden, wenn

1. eine besondere Rechtsvorschrift dies vorsieht,
2. der Betroffene ausdrücklich eingewilligt hat,
3. die Verarbeitung zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist und der Betroffene aus rechtlichen oder tatsächlichen Gründen nicht in der Lage ist, seine Einwilligung zu geben, oder
4. dies zur Geltendmachung rechtlicher Ansprüche vor Gericht einschließlich eines Vorverfahrens erforderlich ist.

(2) Absatz 1 findet keine Anwendung auf die Verarbeitung von Daten über religiöse oder weltanschauliche Überzeugungen nach § 17, von Daten für Zwecke der wissenschaftlichen Forschung nach §§ 19 und 35 und von Daten im Zusammenhang mit Dienst- und Arbeitsverhältnissen nach § 36.

(3) Absatz 1 findet ferner keine Anwendung auf die Verarbeitung personenbezogener Daten

1. zur Gefahrenabwehr,
2. zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen,
3. durch das Landesamt für Verfassungsschutz,
4. durch die Finanzverwaltung, soweit sie die Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung verarbeitet, und

5. bei einer Sicherheitsüberprüfung nach dem Landessicherheitsüberprüfungsgesetz.

§ 33a

Datenverarbeitung in der gemeinsamen Dienststelle

(1) Die örtlich zuständige Stelle darf personenbezogene Daten nur den in einer gemeinsamen Dienststelle nach § 16 des Landesverwaltungsgesetzes beschäftigten eigenen Bediensteten zur Verarbeitung für eigene Aufgaben überlassen. Durch technische und organisatorische Maßnahmen ist sicherzustellen, dass ein Zugriff auf die Daten nach Satz 1 durch Bedienstete anderer Behörden nicht möglich ist. Soweit dies zur Sicherstellung einer sachgerechten Erledigung der eigenen Aufgaben erforderlich ist, darf die örtlich zuständige Stelle auch Bediensteten anderer Behörden, die in der gemeinsamen Dienststelle beschäftigt sind, personenbezogene Daten zur Verarbeitung überlassen. Im Rahmen einer solchen Datenverarbeitung unterliegen die Bediensteten anderer Behörden den Weisungen der örtlich zuständigen Stelle. Hinsichtlich der Daten, die sie im Rahmen ihrer Tätigkeit für die fremde Behörde zur Kenntnis nehmen, haben sie das Datengeheimnis (§ 6) gegenüber ihrer eigenen Dienststelle zu wahren. Das Nähere ist durch gemeinsame interne Dienstanweisungen zu regeln. Verantwortliche Stelle im Sinne des § 3 Abs. 3 bleibt die örtlich zuständige Stelle.

(2) Für gemeinsame Dienststellen nach § 27 des Gesetzes über kommunale Zusammenarbeit gilt Absatz 1 entsprechend.

§ 34

Zweckbindung bei der Verarbeitung personenbezogener Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Person oder Stelle in Ausübung ihrer Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der speichernden Stelle nur für den Zweck verarbeitet werden, für den sie sie erhalten hat. § 33 bleibt unberührt. In die Übermittlung an einen Dritten außerhalb des öffentlichen Bereichs muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet werden, wenn

1. die Änderung des Zwecks durch besonderes Gesetz zugelassen ist oder
2. die Voraussetzungen vorliegen, die eine Nutzung nach § 15 Abs. 1 bis 4 zulassen würden, und die zur Verschwiegenheit verpflichtete Stelle eingewilligt hat.

§ 35

Verarbeitung personenbezogener Daten durch Forschungseinrichtungen

(1) Öffentliche Stellen mit der Aufgabe unabhängiger wissenschaftlicher Forschung dürfen die zur Durchführung wissenschaftlicher Forschung erforderlichen personenbezogenen Daten erheben. Ohne Kenntnis des Betroffenen dürfen die Daten nur erhoben werden, wenn der Zweck des Forschungsvorhabens auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet werden.

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

(3) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, soweit

1. der Betroffene eingewilligt hat oder

2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist und überwiegende schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(4) Bei der Meldung nach § 32 darf die Beschreibung der Zweckbestimmung der Verarbeitung, zu deren Erfüllung personenbezogene Daten verarbeitet werden, auf die Angabe "Forschungsvorhaben" beschränkt werden.

§ 36

Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Personenbezogene Daten von Beschäftigten dürfen nur verarbeitet werden, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift, ein Tarifvertrag oder eine Dienst- oder Betriebsvereinbarung es vorsieht.

(2) Auf die Verarbeitung von Personalaktendaten von Angestellten und Arbeitern sowie Auszubildenden in einem privatrechtlichen Ausbildungsverhältnis finden die für Beamte geltenden Vorschriften des § 50 des Beamtenstatusgesetzes und der §§ 83 bis 88 des Landesbeamtengesetzes entsprechende Anwendung, es sei denn, besondere Rechtsvorschriften oder tarifliche Vereinbarungen gehen vor.

(3) Im Zusammenhang mit der Begründung eines Dienst- oder Arbeitsverhältnisses ist die Erhebung personenbezogener Daten eines Bewerbers bei dem bisherigen Dienstherrn oder Arbeitgeber nur zulässig, wenn der Betroffene eingewilligt hat. Satz 1 gilt entsprechend für die Übermittlung personenbezogener Daten an künftige Dienstherrn oder Arbeitgeber. Steht fest, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt, sind dem Betroffenen die von ihm vorgelegten Unterlagen unverzüglich zurückzusenden und die zu ihm gespeicherten Daten spätestens nach Ablauf eines Jahres zu löschen, es sei denn, er hat in die weitere Verarbeitung eingewilligt oder diese ist wegen eines anhängigen Rechtsstreits erforderlich.

§ 37

Verarbeitung personenbezogener Daten durch den Südwestrundfunk

(1) Soweit der Südwestrundfunk personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen Zwecken verarbeitet, gelten von den Vorschriften dieses Gesetzes neben den Absätzen 2 und 3 und § 38 nur die §§ 6 und 9 sowie § 25 mit der Maßgabe, dass nur für Schäden gehaftet wird, die durch eine Verletzung von § 6 oder § 9 eintreten, entsprechend. Für die Verarbeitung personenbezogener Daten zu anderen Zwecken gelten neben § 38 die Vorschriften dieses Gesetzes entsprechend mit Ausnahme des Vierten Abschnitts. Für Hilfsunternehmen des Südwestrundfunks, die öffentliche Stellen im Sinne des § 2 sind, gelten für die Verarbeitung personenbezogener Daten zu ausschließlich eigenen journalistisch-redaktionellen Zwecken Satz 1 sowie zu anderen Zwecken die Vorschriften dieses Gesetzes entsprechend.

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

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

§ 38

Rundfunkbeauftragter für den Datenschutz

(1) Der Südwestrundfunk bestellt auf die Dauer von acht Jahren einen Rundfunkbeauftragten für den Datenschutz. Die Bestellung erfolgt durch den Rundfunkrat mit Zustimmung des Verwaltungsrats. Die

Dienststelle des Rundfunkbeauftragten für den Datenschutz wird bei der Geschäftsstelle von Rundfunk- und Verwaltungsrat eingerichtet. Dem Rundfunkbeauftragten für den Datenschutz ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen.

(2) Der Rundfunkbeauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung seines Amtes völlig unabhängig und nur dem Gesetz unterworfen. Er unterliegt keiner Rechts- und Fachaufsicht. Der Dienstaufsicht des Verwaltungsrats untersteht er nur insoweit, als seine völlige Unabhängigkeit dadurch nicht beeinträchtigt wird.

(3) Jeder kann sich an den Rundfunkbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch den Südwestrundfunk in seinen Rechten verletzt worden zu sein.

(4) Für Beanstandungen gilt § 30 entsprechend mit der Maßgabe, dass Beanstandungen an den Intendanten unter gleichzeitiger Unterrichtung des Verwaltungsrats zu richten sind. Dem Verwaltungsrat ist auch die zu der Beanstandung abgegebene Stellungnahme des Intendanten zuzuleiten.

(5) Der Rundfunkbeauftragte für den Datenschutz erstattet dem Rundfunkrat und dem Verwaltungsrat alle zwei Jahre einen schriftlichen Bericht über seine Tätigkeit. Der Bericht wird veröffentlicht. Auf Ersuchen des Verwaltungsrats erstattet er dem Verwaltungsrat darüber hinaus besondere Berichte.

(6) Der Rundfunkbeauftragte für den Datenschutz ist auch nach Beendigung seiner Tätigkeit verpflichtet, über die ihm bei seiner dienstlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Er darf ohne Genehmigung des Intendanten über Angelegenheiten im Sinne von Satz 1 weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben.

SECHSTER ABSCHNITT

Übergangs- und Schlussvorschriften

§ 39

(aufgehoben)

§ 40

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer

1. unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,
 - a) speichert, nutzt, verändert, übermittelt oder löscht,
 - b) zum Abruf mittels automatisierten Verfahrens bereithält oder
 - c) abrufen oder sich oder einem anderen aus Dateien verschafft,
2. die Übermittlung von personenbezogenen Daten, die durch dieses Gesetz geschützt werden und nicht offenkundig sind, durch unrichtige Angaben erschleicht,
3. personenbezogene Daten ohne die nach § 18 Abs. 4 Satz 3 oder nach § 34 Abs. 2 Nr. 2 erforderliche Einwilligung oder entgegen § 35 Abs. 1 für einen anderen Zweck nutzt,
4. entgegen § 35 Abs. 2 Satz 3 die in § 35 Abs. 2 Satz 2 bezeichneten Merkmale mit den Einzelangaben zusammenführt oder
5. entgegen § 18 Abs. 5 eine vollziehbare Auflage nicht, nicht rechtzeitig oder nicht vollständig erfüllt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 25 000 Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne von § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten ist das durch Rechtsverordnung des Innenministeriums bestimmte Regierungspräsidium.^{*)}

Fußnoten

* [Gemäß Artikel 8 Absatz 3 des Gesetzes vom 7. Februar 2011 (GBl. S. 43, 46) ist bis zu einer anderweitigen Bestimmung durch Rechtsverordnung des Innenministeriums das Regierungspräsidium Karlsruhe zuständiges Regierungspräsidium.]

§ 41 Straftaten

Wer eine der in § 40 Abs. 1 Nr. 1 bis 4 bezeichneten Handlungen gegen Entgelt oder in der Absicht begeht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Der Versuch ist strafbar.

§ 42¹⁾ Übergangsvorschriften

(aufgehoben)

Fußnoten

1) Diese Vorschriften betreffen §§ 35 bis 42 in der ursprünglichen Fassung vom 27. Mai 1991.

§ 43¹⁾ Änderung des Landesverwaltungsverfahrensgesetzes)

(nicht abgedruckt)

Fußnoten

1) Diese Vorschriften betreffen §§ 35 bis 42 in der ursprünglichen Fassung vom 27. Mai 1991.

§ 44¹⁾ Änderung des Vermessungsgesetzes

(nicht abgedruckt)

Fußnoten

1) Diese Vorschriften betreffen §§ 35 bis 42 in der ursprünglichen Fassung vom 27. Mai 1991.

§ 45¹⁾ Änderung des Landeskatastrophenschutzgesetzes

(nicht abgedruckt)

Fußnoten

1) Diese Vorschriften betreffen §§ 35 bis 42 in der ursprünglichen Fassung vom 27. Mai 1991.

§ 46 ¹⁾
Änderung des Feuerwehrgesetzes

(nicht abgedruckt)

Fußnoten

1) Diese Vorschriften betreffen §§ 35 bis 42 in der ursprünglichen Fassung vom 27. Mai 1991.

§ 47 ¹⁾
**Änderung des Gesetzes zu dem Staatsvertrag
über Bildschirmtext**

(nicht abgedruckt)

Fußnoten

1) Diese Vorschriften betreffen §§ 35 bis 42 in der ursprünglichen Fassung vom 27. Mai 1991.

§ 48 ¹⁾
Änderung des Meldegesetzes

(nicht abgedruckt)

Fußnoten

1) Diese Vorschriften betreffen §§ 35 bis 42 in der ursprünglichen Fassung vom 27. Mai 1991.

§ 49 ¹⁾
Inkrafttreten

(nicht abgedruckt)

Fußnoten

1) Diese Vorschriften betreffen §§ 35 bis 42 in der ursprünglichen Fassung vom 27. Mai 1991.