Inhaltsübersicht:

Abschnitt I

Allgemeine Grundsätze

§ 1

Gesetzeszweck

Zweck dieses Gesetzes ist es, bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen das Recht auf informationelle Selbstbestimmung zu wahren.

§ 2

Begriffsbestimmungen

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

(2) Datenverarbeitung ist die Verwendung personenbezogener Daten. Dabei ist

1. Erheben das Beschaffen von Daten,

2. Speichern das Aufbewahren von Daten auf Datenträgern,

3. Übermitteln das Weitergeben von Daten an Dritte oder der Abruf von zum Abruf bereitgehaltenen Daten durch Dritte,

4. Sperren das Untersagen weiterer Verarbeitung gespeicherter Daten,

5. Löschen das Unkenntlichmachen gespeicherter Daten,

6. Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,

7. Pseudonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse ohne Nutzung der Zuordnungsfunktion nicht oder nur mit einem unverhältnismäßigen Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,

8. Verschlüsseln das Verändern personenbezogener Daten derart, dass ohne Nutzung des Geheimnisses die Kenntnisnahme vom Inhalt der Daten nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist.

(3) Datenverarbeitende Stelle ist jede öffentliche Stelle im Sinne von § 3 Abs. 1, die personenbezogene Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.

(4) Empfänger ist jede natürliche oder juristische Person, öffentliche oder nicht-öffentliche Stelle, die Daten erhält.

(5) Dritte oder Dritter ist jede natürliche oder juristische Person und öffentliche oder nichtöffentliche Stelle außer

1. der datenverarbeitenden Stelle selbst,

2. der betroffenen Person,

3. der Auftragsdatenverarbeiterin oder dem Auftragsdatenverarbeiter und

4. den Personen, die unter der unmittelbaren Verantwortung der datenverarbeitenden Stelle oder der Auftragsdatenverarbeiterin oder des Auftragsdatenverarbeiters befugt sind, die Daten zu verarbeiten.

§ 3

Anwendungsbereich

(1) Dieses Gesetz gilt für öffentliche Stellen. Öffentliche Stellen im Sinne dieses Gesetzes sind

1. Behörden und sonstige öffentliche Stellen der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung,

2. Vereinigungen des privaten Rechts, soweit sie Aufgaben der öffentlichen Verwaltung wahrnehmen und an der Vereinigung einem oder mehreren der im Landesverwaltungsgesetz genannten Träger der öffentlichen Verwaltung die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht.

(2) Soweit öffentlich-rechtliche, der Aufsicht des Landes unterstehende Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, gilt für sie von diesem Gesetz nur § 23; im übrigen gelten für sie die Vorschriften des Bundesdatenschutzgesetzes für nichtöffentliche Stellen.

(3) Soweit besondere Rechtsvorschriften den Umgang mit personenbezogenen Daten regeln, gehen sie den Vorschriften dieses Gesetzes vor.

§ 4

Datenvermeidung und Datensparsamkeit, Datenschutzaudit

(1) Die datenverarbeitende Stelle hat den Grundsatz der Datenvermeidung und Datensparsamkeit zu beachten.

(2) Produkte, deren Vereinbarkeit mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde, sollen vorrangig eingesetzt werden. Die Landesregierung regelt durch Verordnung Inhalt, Ausgestaltung und die Berechtigung zur Durchführung des Verfahrens.

§ 5

Allgemeine Maßnahmen zur Datensicherheit

(1) Die Ausführung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Dabei ist insbesondere

1. Unbefugten der Zugang zu Datenträgern, auf denen personenbezogene Daten gespeichert sind, zu verwehren,

2. zu verhindern, dass personenbezogene Daten unbefugt verarbeitet werden oder Unbefugten zur Kenntnis gelangen können,

3. zu gewährleisten, dass die datenverarbeitende Person, der Zeitpunkt und Umfang der Datenverarbeitung festgestellt werden kann.

(2) Es sind die technischen und organisatorischen Maßnahmen zu treffen, die nach dem Stand der Technik und der Schutzbedürftigkeit der Daten erforderlich und angemessen sind. Automatisierte Verfahren sind vor ihrem erstmaligen Einsatz und nach Änderungen durch die Leiterin oder den Leiter der datenverarbeitenden Stelle oder eine befugte Person freizugeben.

(3) Die Landesregierung regelt durch Verordnung die Anforderungen an das Sicherheitskonzept sowie die Freigabe automatisierter Verfahren und weitere Einzelheiten einer ordnungsgemäßen Datenverarbeitung der öffentlichen Stellen. Das Unabhängige Landeszentrum für Datenschutz ist anzuhören.

§ 6

Besondere Maßnahmen zur Datensicherheit bei Einsatz automatisierter Verfahren

(1) Automatisierte Verfahren sind so zu gestalten, dass eine Verarbeitung personenbezogener Daten erst möglich ist, nachdem die Berechtigung der Benutzerin oder des Benutzers festgestellt worden ist.

(2) Zugriffe, mit denen Änderungen an automatisierten Verfahren bewirkt werden können, dürfen nur den dazu ausdrücklich berechtigten Personen möglich sein. Die Zugriffe dieser Personen sind zu protokollieren und zu kontrollieren.

(3) Werden personenbezogene Daten mit Hilfe informationstechnischer Geräte von der datenverarbeitenden Stelle außerhalb ihrer Räumlichkeiten verarbeitet, sind die Datenbestände zu verschlüsseln. Die datenverarbeitende Stelle hat sicherzustellen, dass sie die Daten entschlüsseln kann.

(4) Sollen personenbezogene Daten ausschließlich automatisiert gespeichert werden, ist zu protokollieren, wann, durch wen und in welcher Weise die Daten gespeichert wurden. Entsprechendes gilt für die Veränderung und Übermittlung der Daten. Die Protokolldatenbestände sind ein Jahr zu speichern. Es ist sicherzustellen, dass die Verfahren und Geräte, mit denen die gespeicherten Daten lesbar gemacht werden können, verfügbar sind.

(5) Die datenverarbeitenden Stellen haben die ordnungsgemäße Anwendung der automatisierten Verfahren zu überwachen.

§ 7

Verfahrensverzeichnis, Meldung

(1) Die datenverarbeitende Stelle erstellt für jedes von ihr betriebene automatisierte Verfahren ein Verfahrensverzeichnis. Dieses Verzeichnis kann auch von einer Stelle für andere geführt werden. Es enthält Angaben über

1. Name und Anschrift der datenverarbeitenden Stelle,

2. Zweckbestimmung und Rechtsgrundlage des Verfahrens,

3. den Kreis der Betroffenen,

4. die Kategorien der verarbeiteten Daten,

5. die Personen und Stellen, die Daten erhalten oder erhalten dürfen einschließlich der Auftragnehmenden,

6. geplante Datenübermittlungen an Stellen außerhalb der Mitgliedstaaten der Europäischen Union,

7. die datenschutzrechtliche Beurteilung der oder des behördlichen Datenschutzbeauftragten, soweit eine solche vorliegt,

8. eine allgemeine Beschreibung der nach den §§ 5 und 6 zur Einhaltung der Datensicherheit getroffenen Maßnahmen.

(2) Absatz 1 gilt nicht für Register, die zur Information der Öffentlichkeit bestimmt sind oder die allen Personen, die mindestens ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen stehen, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

(3) Die datenverarbeitenden Stellen, die keine behördliche Datenschutzbeauftragte oder keinen behördlichen Datenschutzbeauftragten nach § 10 bestellt haben, melden dem Unabhängigen Landeszentrum für Datenschutz den Einsatz oder die wesentliche Änderung eines automatisierten Verfahrens. Ausgenommen sind die in den Absätzen 2 und 4 genannten Verfahren. Die meldepflichtigen Stellen haben spätestens bei der ersten Einspeicherung die Angaben nach Absatz 1 mitzuteilen. Bei Verfahren, die von öffentlichen Stellen entwickelt worden sind, können diese Stellen mit der Abgabe der Meldung beauftragt werden.

(4) Das Unabhängige Landeszentrum für Datenschutz führt ein Verzeichnis der Meldungen nach Absatz 3. Es enthält die Angaben nach Absatz 1. Das Verzeichnis kann von jeder Person eingesehen werden. Satz 3 gilt nicht für Verfahren, die

1. nach dem Landesverfassungsschutzgesetz geführt werden,

2. der Gefahrenabwehr dienen,

3. der Strafverfolgung dienen oder

4. der Steuerfahndung dienen,

soweit die datenverarbeitende Stelle eine Einsichtnahme mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt.

(5) Bei Bestellung einer oder eines behördlichen Datenschutzbeauftragten nach § 10 kann das Verfahrensverzeichnis von jeder Person bei der datenverarbeitenden Stelle eingesehen werden. Die Ausnahmen von der Einsichtnahme nach Absatz 4 Satz 4 gelten entsprechend.

§ 8

Gemeinsame Verfahren und Abrufverfahren

(1) Ein automatisiertes Verfahren, das mehreren datenverarbeitenden Stellen gemeinsam die Verarbeitung personenbezogener Daten (gemeinsames Verfahren) oder die Übermittlung personenbezogener Daten durch Abruf (Abrufverfahren) 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 Verfahrens kontrolliert werden kann. Hierzu ist das Verfahrensverzeichnis nach § 7 Abs. 1 um die Feststellung zu ergänzen, für welchen Bereich der Datenverarbeitung jede der beteiligten Stellen verantwortlich ist. Die Betroffenen können die ihnen nach Abschnitt V dieses Gesetzes zustehenden Rechte gegenüber jeder der beteiligten Stellen geltend machen. Diese leiten die Anliegen der Betroffenen an die nach Satz 2 als verantwortlich festgestellte Stelle weiter.

(3) Werden bei gemeinsamen Verfahren personenbezogene Daten übermittelt, so sind die Empfänger, der Zeitpunkt der Übermittlung und die jeweils übermittelten Daten zu protokollieren. Die Protokolldatenbestände sind ein Jahr zu speichern.

(4) Bei Abrufverfahren trägt die Verantwortung für die Zulässigkeit des einzelnen Abrufs die abrufende Stelle. Die speichernde Stelle prüft die Zulässigkeit des Abrufs nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Zulässigkeit der Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann.

(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.

§ 9

Vorabkontrolle

(1) Vor der Einrichtung oder wesentlichen Änderung

1. eines Verfahrens nach § 8 Abs. 1 oder

2. eines automatisierten Verfahrens, in dem Daten im Sinne des § 11 Abs. 3 verarbeitet werden,

ist der oder dem behördlichen Datenschutzbeauftragten oder, wenn eine solche oder ein solcher nicht bestellt ist, dem Unabhängigen Landeszentrum für Datenschutz Gelegenheit zur Prüfung innerhalb einer angemessenen Frist zu geben, ob die Datenverarbeitung zulässig und die vorgesehenen Maßnahmen nach den §§ 5 und 6 ausreichend sind (Vorabkontrolle).

(2) Absatz 1 gilt nicht für den Abruf aus Datenbeständen, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

§ 10

Behördliche Datenschutzbeauftragte

(1) Die datenverarbeitende Stelle kann schriftlich eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen. Mehrere datenverarbeitende Stellen können gemeinsam eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten bestellen.

(2) Die oder der behördliche Datenschutzbeauftragte muss die erforderliche Sachkunde und Zuverlässigkeit besitzen. Sie oder er darf durch die Bestellung keinem Konflikt mit anderen dienstlichen Aufgaben ausgesetzt sein.

(3) Die oder der behördliche Datenschutzbeauftragte ist unmittelbar der Leiterin oder dem Leiter der datenverarbeitenden Stelle zu unterstellen. Sie oder er ist bei der Ausübung des Amtes weisungsfrei und darf wegen der Wahrnehmung des Amtes nicht benachteiligt werden. Sie oder er ist zur Erfüllung der Aufgaben des Amtes im erforderlichen Umfang freizustellen und mit den notwendigen Mitteln auszustatten. Beschäftigte und Betroffene können sich ohne Einhaltung des Dienstweges in allen Angelegenheiten des Datenschutzes an sie oder ihn wenden. Die oder der behördliche Datenschutzbeauftragte darf zur Aufgabenerfüllung Einsicht in personenbezogene Datenverarbeitungsvorgänge nehmen. Dies gilt nicht, soweit besondere Amts- und Berufsgeheimnisse dem entgegenstehen. Im übrigen gilt § 41 Abs. 1 entsprechend.

(4) Die oder der behördliche Datenschutzbeauftragte überwacht und unterstützt die Einhaltung der datenschutzrechtlichen Vorschriften bei der datenverarbeitenden Stelle. Sie oder er hat insbesondere

1. auf die Einhaltung der Datenschutzvorschriften bei der Einführung von Datenverarbeitungsmaßnahmen hinzuwirken,

2. die Beschäftigten der datenverarbeitenden Stellen mit den Bestimmungen dieses Gesetzes sowie den sonstigen Vorschriften über den Datenschutz vertraut zu machen,

3. die datenverarbeitende Stelle bei der Gestaltung und Auswahl von Verfahren zur Verarbeitung personenbezogener Daten zu beraten und bei der Einführung neuer Verfahren oder der Änderung bestehender Verfahren auf die Einhaltung der einschlägigen Vorschriften hinzuwirken,

4. das Verzeichnis nach § 7 Abs. 1 zu führen und zur Einsicht bereitzuhalten,

5. die Vorabkontrolle nach § 9 Abs. 1 durchzuführen.

In Zweifelsfällen hat sie oder er das Unabhängige Landeszentrum für Datenschutz zu hören.

Abschnitt II

Zulässigkeit der Datenverarbeitung

§ 11

Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist zulässig, wenn

1. die oder der Betroffene eingewilligt hat,

2. dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt,

3. sie zur rechtmäßigen Erfüllung der durch Rechtsvorschrift zugewiesenen Aufgaben der datenverarbeitenden Stelle erforderlich ist oder

4. sie zur Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist.

(2) Die Verarbeitung personenbezogener Daten, die allgemein zugänglichen Quellen entnommen werden können, sowie von Daten, die die Betroffenen selbst zur Veröffentlichung bestimmt haben, ist über die Fälle von Absatz 1 hinaus zulässig, soweit schutzwürdige Belange der Betroffenen nicht beeinträchtigt sind.

(3) Die Verarbeitung personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben sowie von Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen, ist nur zulässig, soweit

1. die oder der Betroffene eingewilligt hat,

2. die Voraussetzungen des § 17 Abs. 5 oder der §§ 22 bis 25 vorliegen,

3. andere Rechtsvorschriften sie erlauben,

4. sie ausschließlich im Interesse der oder des Betroffenen liegt,

5. sie sich auf Daten bezieht, die die oder der Betroffene selbst öffentlich gemacht hat,

6. sie zur Geltendmachung rechtlicher Ansprüche vor Gericht erforderlich ist oder

7. sie für die Abwehr von Gefahren für Leben, Gesundheit, persönliche Freiheit oder vergleichbare Rechtsgüter erforderlich ist.

Satz 1 gilt entsprechend für Daten über strafbare Handlungen und Entscheidungen in Strafsachen.

(4) Die Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. Sind personenbezogene Daten in Akten derart verbunden, dass ihre Trennung nach erforderlichen und nicht erforderlichen Daten auch durch Vervielfältigung und Unkenntlichmachung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, so sind auch die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, zulässig, soweit nicht schutzwürdige Belange der oder des Betroffenen überwiegen. Die nicht erforderlichen Daten unterliegen insoweit einem Verwertungsverbot.

(5) Die Absätze 3 und 4 finden keine Anwendung, wenn die Datenverarbeitung

1. durch die Verfassungsschutzbehörde zur Erfüllung ihrer Aufgaben erfolgt,

2. der Gefahrenabwehr dient,

3. der Strafverfolgung dient oder

4. der Steuerfahndung dient.

Absatz 3 Satz 1 findet keine Anwendung, wenn die Datenverarbeitung der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder der Verwaltung von

Gesundheitsdiensten dient und die Verarbeitung der Daten durch ärztliches Personal oder sonstige Personen, die einer der ärztlichen Schweigepflicht entsprechenden Geheimhaltungspflicht unterliegen, erfolgt.

(6) Pseudonymisierte Daten dürfen nur von solchen Stellen verarbeitet werden, die keinen Zugriff auf die Zuordnungsfunktion haben. Die Übermittlung pseudonymisierter Daten ist zulässig, wenn die Zuordnungsfunktion im alleinigen Zugriff der übermittelnden Stelle verbleibt.

§ 12

Form der Einwilligung

(1) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. In den Fällen des § 11 Abs. 3 muss sich die Einwilligung ausdrücklich auf die dort aufgeführten Daten beziehen. Soll die Einwilligung zusammen mit anderen Erklärungen erteilt werden, ist die oder der Betroffene auf die Einwilligungserklärung schriftlich besonders hinzuweisen.

(2) Die oder der Betroffene ist in geeigneter Weise über die Bedeutung der Einwilligung aufzuklären. Dabei ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass die Einwilligung verweigert und mit Wirkung für die Zukunft widerrufen werden kann.

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

1. sie nur durch eine eindeutige und bewusste Handlung der oder des Betroffenen erfolgen kann,

2. sie nicht unerkennbar verändert werden kann,

3. ihre Urheberin oder ihr Urheber erkannt werden kann und

4. die Einwilligung bei der verarbeitenden Stelle protokolliert wird.

§ 13

Erhebung, Zweckbindung

(1) Personenbezogene Daten sind bei den Betroffenen mit ihrer Kenntnis zu erheben. Ohne Kenntnis der Betroffenen dürfen personenbezogene Daten nur erhoben werden, wenn die Voraussetzungen von Absatz 3 Nr. 1, 2 oder 4 vorliegen. Die Herkunft der Daten ist zu dokumentieren.

(2) Personenbezogene Daten dürfen nur für den Zweck weiterverarbeitet werden, für den sie rechtmäßig erhoben worden sind. Daten, von denen die öffentliche Stelle ohne Erhebung Kenntnis erlangt hat, dürfen nur für die Zwecke weiterverarbeitet werden, für die sie erstmals rechtmäßig gespeichert worden sind.

(3) Die Verarbeitung für andere Zwecke ist ohne Einwilligung der oder des Betroffenen nur zulässig, wenn

1. eine Rechtsvorschrift dies erlaubt,

2. die Abwehr erheblicher Nachteile für das Allgemeinwohl oder von Gefahren für Leben, Gesundheit, persönliche Freiheit oder sonstiger schwerwiegender Beeinträchtigungen der Rechte einzelner dies gebietet,

3. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben oder

4. die Einholung der Einwilligung nicht oder nur mit unverhältnismäßigem Aufwand möglich wäre und offensichtlich ist, dass die Verarbeitung im Interesse der oder des Betroffenen liegt und sie oder er in Kenntnis des anderen Zwecks die Einwilligung erteilen würde.

(4) Daten im Sinne von § 11 Abs. 3 Satz 1 dürfen ohne Einwilligung der oder des Betroffenen für andere Zwecke nur verarbeitet werden, wenn die Voraussetzungen des Absatzes 3 Nr. 1 oder 2 vorliegen. Dies gilt nicht in den Fällen des § 11 Abs. 5.

(5) Die Verarbeitung der Daten zur Ausübung von Aufsichts- und Kontrollbefugnissen sowie zur Rechnungsprüfung gilt nicht als Verarbeitung für andere Zwecke. Daten, die zu einem anderen Zweck erhoben oder erstmalig gespeichert wurden, sind für Ausbildungs- und Prüfungszwecke in anonymisierter oder pseudonymisierter Form zu verarbeiten. Lassen sich die in Satz 2 genannten Zwecke durch anonymisierte oder pseudonymisierte Datenverarbeitung nicht erreichen, so ist die Zweckänderung zulässig, soweit berechtigte Interessen der oder des Betroffenen an der Geheimhaltung der Daten nicht überwiegen.

(6) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherheit oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

(7) Werden Daten innerhalb einer datenverarbeitenden Stelle zu einem anderen Zweck als dem nach Absatz 2 weiterverarbeitet, so ist dies zu dokumentieren.

§ 14

Datenübermittlung an andere öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an andere öffentliche Stellen ist zulässig, wenn die Voraussetzungen der §§ 11 und 13 Abs. 2 bis 6 vorliegen.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Soll die Übermittlung auf Ersuchen einer Stelle erfolgen, so hat diese die hierfür erforderlichen Angaben zu machen, insbesondere die Rechtsgrundlage für die Übermittlung anzugeben. Die übermittelnde Stelle prüft die Schlüssigkeit der Anfrage. Bestehen im Einzelfall Zweifel, so prüft sie auch die Rechtmäßigkeit des Ersuchens.

§ 15

Datenübermittlung an nichtöffentliche Stellen

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

1. von diesen ein rechtliches Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft gemacht wird und schutzwürdige Belange der oder des Betroffenen nicht beeinträchtigt sind oder

2. die Voraussetzungen der §§ 11 und 13 Abs. 2 bis 6 vorliegen.

(2) Die übermittelnde Stelle hat die empfangende Stelle zu verpflichten, die Daten nur zu dem Zweck zu verwenden, zu dem sie ihr übermittelt wurden.

§ 16

Datenübermittlung an ausländische Stellen

(1) Die Zulässigkeit der Übermittlung an öffentliche und nichtöffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes richtet sich nach den §§ 14 und 15.

(2) Die Übermittlung an Stellen außerhalb der Mitgliedstaaten der Europäischen Union ist nur zulässig, wenn dort ein angemessenes Datenschutzniveau gewährleistet ist. Fehlt es an einem angemessenen Datenschutzniveau, so ist die Übermittlung nur zulässig, wenn

1. die oder der Betroffene eingewilligt hat,

2. die Übermittlung zur Wahrung eines überwiegenden öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung eines rechtlichen Interesses erforderlich ist,

3. die Übermittlung zur Wahrung lebenswichtiger Interessen der oder des Betroffenen erforderlich ist,

4. die Übermittlung aus einem für die Öffentlichkeit bestimmten Register erfolgt oder

5. die empfangende Stelle ausreichende Garantien hinsichtlich des Schutzes der Grundrechte bietet.

(3) Vor der Entscheidung über die Angemessenheit des Datenschutzniveaus und einer Entscheidung nach Absatz 2 Nr. 5 ist das Unabhängige Landeszentrum für Datenschutz zu hören.

(4) Die empfangende Stelle ist darauf hinzuweisen, dass die Daten nur zu den Zwecken verarbeitet werden dürfen, für die sie übermittelt wurden.

Abschnitt III

Besondere Formen der Datenverarbeitung

§ 17

Verarbeitung personenbezogener Daten im Auftrag, Wartung

(1) Lässt eine datenverarbeitende Stelle personenbezogene Daten in ihrem Auftrag verarbeiten, bleibt sie für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Rechte der Betroffenen sind ihr gegenüber geltend zu machen. Die Weitergabe der Daten von der datenverarbeitenden Stelle an die Auftragnehmenden gilt nicht als Übermittlung im Sinne von § 2 Abs. 2 Nr. 3.

(2) Die datenverarbeitende Stelle hat dafür Sorge zu tragen, dass personenbezogene Daten nur im Rahmen ihrer Weisungen verarbeitet werden. Sie hat die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um dies sicherzustellen. Sie hat Auftragnehmende unter besonderer Berücksichtigung ihrer Eignung für die Gewährleistung der nach den §§ 5 und 6 notwendigen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Aufträge, ergänzende Weisungen zu technischen und organisatorischen Maßnahmen und die etwaige Zulässigkeit von Unterauftragsverhältnissen sind schriftlich festzulegen.

(3) Sofern die Vorschriften dieses Gesetzes auf Auftragnehmende keine Anwendung finden, hat die datenverarbeitende Stelle diese zu verpflichten, jederzeit von ihr veranlasste Kontrollen zu ermöglichen.

(4) Bei der Erbringung von Wartungsarbeiten oder von vergleichbaren Unterstützungstätigkeiten bei der Datenverarbeitung durch Stellen oder Personen außerhalb der datenverarbeitenden Stelle gelten die Absätze 1 bis 3 entsprechend.

(5) Zur Durchführung von beratenden oder begutachtenden Tätigkeiten im Auftrag der datenverarbeitenden Stelle ist die Übermittlung personenbezogener Daten zulässig, wenn die übermittelnde Stelle die beauftragten Personen verpflichtet,

1. die Daten nur zu dem Zweck zu verarbeiten, zu dem sie ihnen überlassen worden sind und

2. nach Erledigung des Auftrags die ihnen von der datenverarbeitenden Stelle überlassenen Datenträger zurückzugeben und die bei ihnen gespeicherten Daten zu löschen, soweit nicht besondere Rechtsvorschriften entgegenstehen.

Die Absätze 1 bis 3 gelten entsprechend.

§ 18

Mobile personenbezogene Datenverarbeitungssysteme

(1) Mobile personenbezogene Speicher- und Verarbeitungsmedien zum Einsatz in automatisierten Verfahren, die an die Betroffenen ausgegeben werden und die über eine von der ausgebenden Stelle oder Dritten bereitgestellte Schnittstelle Daten der Betroffenen automatisiert austauschen können (mobile Datenverarbeitungssysteme, z.B. Chipkarten), dürfen nur mit der Einwilligung der oder des Betroffenen oder aufgrund einer Rechtsvorschrift eingesetzt werden.

(2) Für die Betroffenen muss jederzeit erkennbar sein,

1. ob Datenverarbeitungsvorgänge auf dem mobilen Datenverarbeitungssystem oder durch dieses veranlasst stattfinden,

2. welche personenbezogenen Daten der oder des Betroffenen verarbeitet werden und

3. welcher Verarbeitungsvorgang im einzelnen abläuft oder angestoßen wird.

(3) Die Betroffenen sind bei der Ausgabe des mobilen Datenverarbeitungssystems über die ihnen nach den §§ 26 ff. zustehenden Rechte aufzuklären.

§ 19

Automatisierte Einzelentscheidungen

Entscheidungen, die zu einer tatsächlichen oder rechtlichen Beschwer der Betroffenen führen, dürfen nicht ausschließlich auf die Ergebnisse automatisierter Verfahren, die einzelne Aspekte der Person der Betroffenen bewerten, gestützt werden. Ergebnisse automatisierter Verfahren dürfen abweichend von Satz 1 für Entscheidungen verwendet werden, wenn

1. ein Gesetz dies vorsieht oder

2. der oder dem Betroffenen vor der Entscheidung ermöglicht wird, ihre oder seine besonderen persönlichen Interessen geltend zu machen.

§ 20

Video-Überwachung und -Aufzeichnung

(1) Öffentliche Stellen dürfen mit optisch-elektronischen Einrichtungen öffentlich zugängliche Räume beobachten (Video-Überwachung), soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrnehmung eines Hausrechts erforderlich ist und schutzwürdige Belange Betroffener nicht überwiegen.

(2) Das Bildmaterial darf gespeichert werden (Video-Aufzeichnung), wenn die Tatsache der Aufzeichnung für die Betroffenen durch geeignete Maßnahmen erkennbar gemacht ist. Die Aufzeichnungen sind spätestens nach sieben Tagen zu löschen, es sei denn, sie dokumentieren Vorkommnisse, zu deren Aufklärung die weitere Speicherung erforderlich ist.

§ 21

Fernmessen und Fernwirken

(1) Wer eine Datenverarbeitungs- oder Übertragungseinrichtung zu dem Zweck nutzt, bei einem Betroffenen, insbesondere in der Wohnung oder in den Geschäftsräumen ferngesteuert Messungen vorzunehmen oder andere Wirkungen auszulösen, bedarf dessen Einwilligung.

(2) Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses darf nicht von der Einwilligung der oder des Betroffenen nach Absatz 1 abhängig gemacht werden. Verweigert oder widerruft die oder der Betroffene ihre oder seine Einwilligung, so dürfen ihr oder ihm keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

Abschnitt IV

Besondere Zwecke der Datenverarbeitung

§ 22

Datenverarbeitung für wissenschaftliche Zwecke

(1) Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken durch öffentliche Stellen und die Übermittlung personenbezogener Daten durch öffentliche Stellen an Dritte, die die Daten zu wissenschaftlichen Zwecken nutzen wollen (Datenverarbeitung für wissenschaftliche Zwecke), soll in anonymisierter Form erfolgen. Ist eine Anonymisierung nicht möglich, sollen die Daten pseudonymisiert werden. § 11 Abs. 6 gilt entsprechend.

(2) Steht bei der übermittelnden Stelle zur Erfassung der Daten, zur Anonymisierung oder Pseudonymisierung nicht ausreichend Personal zur Verfügung, so können die mit der Forschung

befassten Personen diese Aufgaben wahrnehmen, wenn sie zuvor zur Verschwiegenheit verpflichtet worden sind.

(3) Ist weder eine Anonymisierung noch eine Pseudonymisierung möglich, ist die Datenverarbeitung für wissenschaftliche Zwecke zulässig, wenn

1. die oder der Betroffene in die Datenverarbeitung eingewilligt hat,

2. es sich nicht um Daten nach § 11 Abs. 3 handelt und schutzwürdige Belange der oder des Betroffenen wegen der Art der Daten oder wegen der Art der Verwendung für das jeweilige Forschungsvorhaben nicht beeinträchtigt sind oder

3. die Genehmigung der für die datenverarbeitende Stelle zuständigen obersten Aufsichtsbehörde vorliegt.

(4) Die Genehmigung nach Absatz 3 Nr. 3 wird erteilt, wenn das öffentliche Interesse an der Durchführung des jeweiligen Forschungsvorhabens die schutzwürdigen Belange der oder des Betroffenen erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Die Genehmigung muss den Forschungszweck, die Art der zu verarbeitenden Daten, den Kreis der Betroffenen sowie bei Übermittlungen den Empfängerkreis bezeichnen und ist dem Unabhängigen Landeszentrum für Datenschutz mitzuteilen.

(5) Sobald der Forschungszweck es gestattet, sind die Daten zu anonymisieren, hilfsweise zu pseudonymisieren. Nach Maßgabe der Absätze 1 bis 3 dürfen die personenbezogenen Daten auch für einen anderen als den ursprünglichen Forschungszweck weiterverarbeitet werden.

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

1. die oder der Betroffene eingewilligt hat oder

2. dies für die Darstellung von Forschungsergebnissen über Personen der Zeitgeschichte unerlässlich ist.

(7) Die übermittelnde Stelle hat empfangende Stellen, auf die dieses Gesetz keine Anwendung findet, zu verpflichten, die Vorschriften der Absätze 5 und 6 einzuhalten und jederzeit Kontrollen durch das Unabhängige Landeszentrum für Datenschutz zu ermöglichen.

§ 23

Datenverarbeitung bei Dienst- und Arbeitsverhältnissen

(1) Öffentliche Stellen dürfen Daten der Beschäftigten vorbehaltlich besonderer gesetzlicher oder tarifvertraglicher Regelungen nur nach Maßgabe der §§ 85 bis 92 des Landesbeamtengesetzes verarbeiten.

(2) Daten von Beschäftigten, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach den §§ 5 und 6 gespeichert oder in einem automatisierten Verfahren gewonnen werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle ausgewertet werden.

§ 24

Öffentliche Auszeichnungen

(1) Zur Vorbereitung öffentlicher Auszeichnungen dürfen die Ministerpräsidentin oder der Ministerpräsident, das Innenministerium sowie die von der Ministerpräsidentin oder dem Ministerpräsidenten besonders beauftragten Stellen die dazu erforderlichen personenbezogenen Daten auch ohne Kenntnis der Betroffenen erheben und weiterverarbeiten. Eine Verarbeitung dieser Daten für andere Zwecke ist nur mit Einwilligung der Betroffenen zulässig.

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

(3) § 27 findet keine Anwendung.

§ 25

Besondere Dokumentationsstelle für Sekten

(1) Die Ministerpräsidentin oder der Ministerpräsident oder eine von ihr oder von ihm besonders beauftragte Stelle (Dokumentationsstelle) kann zum Zweck der Aufklärung oder Warnung die Betätigungen von Sekten oder sektenähnlichen Vereinigungen einschließlich der mit ihnen rechtlich, wirtschaftlich oder in ihrer religiösen oder weltanschaulichen Zielsetzung verbundenen Organisationen oder Vereinigungen in Schleswig-Holstein dokumentieren und über sie informieren, sofern tatsächliche Anhaltspunkte den Verdacht begründen, dass von deren Wirken Gefahren für die Menschenwürde, die freie Entfaltung der Persönlichkeit, das Leben, die Gesundheit oder das Eigentum ausgehen, insbesondere dass Personen in ihrer Willensfreiheit eingeschränkt werden.

(2) Soweit ein begründeter Verdacht im Sinne des Absatz 1 besteht, kann die Dokumentationsstelle über Personen, die in einer derartigen Sekte, Vereinigung oder Organisation aktiv mitwirken, bei anderen öffentlichen Stellen vorhandene oder öffentlich zugängliche personenbezogene Daten erheben und weiterverarbeiten. Hiervon ausgenommen sind Daten, die besonderen Berufs- oder Amtsgeheimnissen unterliegen, sowie Daten, für die besondere Verwendungsvorschriften in anderen Gesetzen bestehen.

(3) Die Speicherung der erhobenen personenbezogenen Daten ist spätestens nach zwei Jahren auf ihre Erforderlichkeit zu prüfen. Spätestens fünf Jahre nach der letzten Tätigkeit im Sinne von Absatz 2 sind die personenbezogenen Daten zu löschen.

(4) An Stellen außerhalb des öffentlichen Bereichs dürfen personenbezogene Daten übermittelt werden, wenn

1. es zur Erfüllung der Aufgabe nach Absatz 1 erforderlich ist oder

2. ein Dritter ein rechtliches Interesse daran hat

und schutzwürdige Belange der oder des Betroffenen nicht beeinträchtigt sind.

Abschnitt V

Rechte der Betroffenen

§ 26

Aufklärung, Benachrichtigung

(1) Werden personenbezogene Daten bei den Betroffenen mit ihrer Kenntnis erhoben, so sind sie in geeigneter Weise über die datenverarbeitende Stelle und den Zweck der Datenverarbeitung aufzuklären. Die Betroffenen sind darüber hinaus aufzuklären über

1. die Rechtsvorschrift, die die Datenverarbeitung gestattet; liegt eine solche nicht vor, die Freiwilligkeit der Datenangabe,

2. die Folgen einer Nichtbeantwortung, wenn die Angaben für die Gewährung einer Leistung erforderlich sind,

3. ihre Rechte nach diesem Gesetz,

4. den Empfängerkreis bei beabsichtigten Übermittlungen sowie

5. die Auftragnehmenden bei beabsichtigter Datenverarbeitung im Auftrag,

soweit es nach den Umständen des Einzelfalles angemessen erscheint. Die Pflicht zur Benachrichtigung nach den Sätzen 1 und 2 entfällt, wenn den Betroffenen die Informationen bereits vorliegen.

(2) Absatz 1 gilt nicht für

1. die Verfassungsschutzbehörden,

2. die Behörden der Staatsanwaltschaft,

3. die Behörden der Polizei,

4. die Gefahrenabwehrbehörden und

5. die Landesfinanzverwaltungen.

(3) Werden die Daten ohne Kenntnis der Betroffenen erhoben, so sind diese in angemessener Weise über die verarbeiteten Daten und über die in Absatz 1 Satz 1 und Satz 2 Nr. 1 und 3 bis 5 genannten Umstände zu unterrichten. Eine Pflicht zur Aufklärung besteht nicht, wenn die Benachrichtigung der Betroffenen unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert. Sollen die Daten übermittelt werden, so hat die Benachrichtigung spätestens zeitgleich mit der Übermittlung zu erfolgen. Satz 1 und 3 finden keine Anwendung, wenn die Betroffenen auf andere Weise Kenntnis von der Verarbeitung ihrer Daten erlangt haben.

§ 27

Auskunft an Betroffene

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

1. die zu ihrer Person gespeicherten Daten,

2. den Zweck und die Rechtsgrundlage der Speicherung,

3. die Herkunft der Daten und den Empfängerkreis von Übermittlungen,

4. die Auftragnehmenden bei Datenverarbeitung im Auftrag,

5. die Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den gesetzlichen Bestimmungen entspricht, insbesondere wenn diese Daten unvollständig oder unrichtig sind, sowie

6. die Funktionsweise von automatisierten Verfahren.

Die Betroffenen sollen die Art der personenbezogenen Daten, über die Auskunft verlangt wird, näher bezeichnen.

(2) Den Betroffenen kann statt der Auskunft Einsicht in die zu ihrer Person gespeicherten Daten gewährt werden. Die Einsicht wird nicht gewährt, soweit diese mit personenbezogenen Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Rechtsvorschriften über die Akteneinsicht im Verwaltungsverfahren bleiben unberührt.

(3) Die Auskunftserteilung oder die Gewährung von Einsicht unterbleibt, soweit eine Prüfung ergibt, dass

1. dadurch die Erfüllung der Aufgaben der datenverarbeitenden Stelle, einer übermittelnden Stelle oder einer empfangenden Stelle gefährdet würde,

2. dadurch die öffentliche Sicherheit gefährdet würde oder sonst dem Wohle des Bundes oder eines Landes schwere Nachteile entstehen würden oder

3. die personenbezogenen Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder wegen der berechtigten Interessen einer dritten Person geheimgehalten werden müssen.

(4) Werden Auskunft oder Einsicht nicht gewährt, ist die oder der Betroffene unter Mitteilung der wesentlichen Gründe darauf hinzuweisen, dass sie oder er sich an das Unabhängige Landeszentrum für Datenschutz wenden kann. Eine Begründung für die Auskunftsverweigerung erfolgt nicht, soweit dadurch der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde.

§ 28

Berichtigung, Löschung, Sperrung

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.

(2) Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder

2. ihre Kenntnis für die datenverarbeitende Stelle zur Aufgabenerfüllung nicht mehr erforderlich ist.

Die datenverarbeitende Stelle legt in allgemeinen Regelungen über die Aufbewahrung von Daten den Zeitraum fest, innerhalb dessen die Daten als zur Aufgabenerfüllung erforderlich gelten. Sind personenbezogene Daten in Akten untrennbar im Sinne von § 11 Abs. 4 Satz 2 gespeichert, ist die Löschung nur durchzuführen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist.

(3) Personenbezogene Daten sind zu sperren, wenn

1. ihre Richtigkeit von der oder dem Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit nachweisen lässt,

2. sie zur Aufgabenerfüllung nicht mehr erforderlich sind, Rechtsvorschriften jedoch die weitere Aufbewahrung anordnen,

3. die oder der Betroffene anstelle der Löschung die Sperrung verlangt,

4. die Löschung die Betroffene oder den Betroffenen in der Verfolgung ihrer oder seiner Rechte oder in sonstigen schutzwürdigen Belangen beeinträchtigen würde oder

5. eine Löschung gemäß Absatz 2 Satz 3 nicht erfolgt.

(4) Gesperrte Daten dürfen über die Speicherung hinaus ohne Einwilligung der oder des Betroffenen nicht mehr weiterverarbeitet werden, es sei denn, dass Rechtsvorschriften die Verarbeitung zulassen oder die Nutzung durch die datenverarbeitende Stelle zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der datenverarbeitenden Stelle oder von Dritten liegenden Gründen unerlässlich ist. Die Gründe für die Nutzung gesperrter Daten sind zu dokumentieren.

(5) Von der Berichtigung, Sperrung oder Löschung nach Absatz 2 Nr. 1 sind unverzüglich die Stellen zu unterrichten, denen die Daten übermittelt wurden. Die Unterrichtung kann unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde und schutzwürdige Belange der oder des Betroffenen nicht beeinträchtigt werden.

§ 29

Einwand gegen die Verarbeitung

(1) Die Betroffenen haben das Recht, schriftlich unter Hinweis auf besondere persönliche Gründe Einwand gegen die Verarbeitung ihrer Daten allgemein oder gegen bestimmte Formen der Verarbeitung zu erheben. Der Einwand ist begründet, wenn ein schutzwürdiges Interesse der oder des Betroffenen das öffentliche Interesse an der Datenverarbeitung im Einzelfall überwiegt. In diesem Fall ist die Datenverarbeitung insgesamt oder in bestimmten Formen unzulässig.

(2) Absatz 1 findet keine Anwendung bei Verfahren, die

1. nach dem Landesverfassungsschutzgesetz geführt werden,

2. der Gefahrenabwehr dienen,

3. der Strafverfolgung dienen oder

4. der Steuerfahndung dienen.

§ 30

Schadensersatz

(1) Entsteht der oder dem Betroffenen durch eine unzulässige oder unrichtige Verarbeitung ihrer oder seiner personenbezogenen Daten in einem automatisierten Verfahren ein Schaden, so ist ihr oder ihm der Träger jeder für die Verarbeitung verantwortlichen Stelle unabhängig von einem Verschulden zum Schadensersatz verpflichtet.

(2) In Fällen einer schweren Verletzung des Persönlichkeitsrechts kann die oder der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen.

(3) Die ersatzpflichtige Stelle haftet jeder oder jedem Betroffenen für jedes schädigende Ereignis bis zu einem Betrag von 125.000 Euro. Mehrere Ersatzpflichtige haften gesamtschuldnerisch.

(4) Auf das Mitverschulden der oder des Betroffenen und die Verjährung des Entschädigungsanspruchs sind die §§ 254, 839 Abs. 3 , §§ 195 und 199 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(5) Die Geltendmachung weitergehender Schadensersatzansprüche aufgrund anderer Vorschriften bleibt unberührt.

§ 31

Unabdingbarkeit

Die Rechte der Betroffenen aus diesem Gesetz können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

Abschnitt VI

Das Unabhängige Landeszentrum für Datenschutz

§ 32

Errichtung und Rechtsform

(1) Das Land Schleswig-Holstein errichtet unter dem Namen "Unabhängiges Landeszentrum für Datenschutz" eine rechtsfähige Anstalt des öffentlichen Rechts. Sitz der Anstalt ist die Landeshauptstadt Kiel.

(2) Die Anstalt besitzt Dienstherrnfähigkeit und führt das kleine Landessiegel.

§ 33

Trägerschaft, Anstaltslast und Gewährträgerhaftung

(1) Träger der Anstalt ist das Land Schleswig-Holstein.

(2) Für Verbindlichkeiten der Anstalt haftet der Anstaltsträger Dritten gegenüber, soweit nicht eine Befriedigung aus dem Vermögen der Anstalt möglich ist.

(3) Der Anstaltsträger stellt sicher, dass die Anstalt ihre gesetzlichen Aufgaben erfüllen kann.

§ 34

Organ

(1) Organ der Anstalt ist der Vorstand.

(2) Der Vorstand besteht aus der Leiterin oder dem Leiter der Anstalt. Sie oder er führt die Bezeichnung "Landesbeauftragte für Datenschutz" oder "Landesbeauftragter für Datenschutz".

(3) Die Landesbeauftragte oder der Landesbeauftragte für Datenschutz führt die Geschäfte der Anstalt und vertritt sie gerichtlich und außergerichtlich. In ihrem oder seinem Verhinderungsfalle vertritt die oder der stellvertretende Landesbeauftragte für Datenschutz die Anstalt und führt deren Geschäfte.

§ 35

Wahl und Amtszeit der oder des Landesbeauftragten für Datenschutz

(1) Der Landtag wählt ohne Aussprache die Landesbeauftragte oder den Landesbeauftragten für Datenschutz mit mehr als der Hälfte seiner Mitglieder für die Dauer von fünf Jahren. Die Wiederwahl ist nur einmal zulässig.

(2) Vorschlagsberechtigt sind die Fraktionen des Schleswig-Holsteinischen Landtages. Kommt vor Ablauf der Amtszeit eine Neuwahl nicht zustande, führt die oder der Landesbeauftragte für Datenschutz das Amt bis zur Neuwahl weiter.

(3) Der Landtag kann die Landesbeauftragte oder den Landesbeauftragten für Datenschutz mit einer Mehrheit von zwei Dritteln seiner Mitglieder abwählen.

§ 36

Rechtsstellung der oder des Landesbeauftragten für Datenschutz

(1) Die Ministerpräsidentin oder der Ministerpräsident ernennt die Landesbeauftragte oder den Landesbeauftragten zur Beamtin oder zum Beamten auf Zeit.

(2) Die oder der Landesbeauftragte für Datenschutz kann jederzeit die Entlassung verlangen.

(3) Die Ministerpräsidentin oder der Ministerpräsident ist Dienstvorgesetzte oder Dienstvorgesetzter der oder des Landesbeauftragten für Datenschutz. Die oder der Landesbeauftragte für Datenschutz untersteht der Dienstaufsicht nur, soweit nicht seine Unabhängigkeit bei der Aufgabenwahrnehmung beeinträchtigt wird.

(4) Der Landtag und seine Ausschüsse können die Anwesenheit der oder des Landesbeauftragten für Datenschutz in ihren Sitzungen verlangen.

(5) Die oder der Landesbeauftragte für Datenschutz ist Dienstvorgesetzte oder Dienstvorgesetzter und oberste Dienstbehörde der in der Anstalt beschäftigten Beamtinnen und Beamten.

(6) Die oder der Landesbeauftragte für Datenschutz bestellt eine Mitarbeiterin zur Stellvertreterin oder einen Mitarbeiter zum Stellvertreter und ernennt die Beamtinnen oder Beamten der Anstalt.

§ 37

Satzung

Der Vorstand ist zum Erlass und zur Änderung der Satzung befugt.

§ 38

Beirat

Der Vorstand kann einen Beirat berufen, der den Vorstand der Anstalt berät. Das Nähere regelt die Satzung.

§ 39

Aufgaben des Unabhängigen Landeszentrums für Datenschutz

(1) Das Unabhängige Landeszentrum für Datenschutz nimmt die ihm zugewiesenen Aufgaben in Unabhängigkeit wahr und ist nur dem Gesetz unterworfen. Die §§ 50 bis 52 des Landesverwaltungsgesetzes sind nicht anzuwenden; im Übrigen sind die Rechtsvorschriften, die für die der Aufsicht des Landes unterstehenden rechtsfähigen Anstalten des öffentlichen Rechts gelten, anzuwenden.

(2) Das Unabhängige Landeszentrum für Datenschutz überwacht die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den öffentlichen Stellen, auf die dieses Gesetz Anwendung findet. Die Gerichte und der Landesrechnungshof unterliegen seiner Kontrolle, soweit sie nicht in richterlicher Unabhängigkeit tätig werden.

(3) Das Unabhängige Landeszentrum für Datenschutz ist die zuständige Aufsichtsbehörde nach § 38 des Bundesdatenschutzgesetzes über nichtöffentliche Stellen im Anwendungsbereich des Dritten Abschnitts des Bundesdatenschutzgesetzes.

(4) Das Unabhängige Landeszentrum für Datenschutz berät die obersten Landesbehörden sowie die sonstigen öffentlichen Stellen in Fragen des Datenschutzes, der Datensicherheit und der damit zusammenhängenden Datenverarbeitungstechniken sowie deren Sozialverträglichkeit. Zu diesem Zweck können Empfehlungen zur Verbesserung des Datenschutzes gegeben werden. Auf Anforderungen des Landtages, des Petitionsausschusses des Landtages oder einer obersten Landesbehörde soll das Unabhängige Landeszentrum für Datenschutz ferner Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenbereich unmittelbar betreffen, nachgehen.

(5) Auf Anforderung des Landtages, einzelner Fraktionen des Landtages oder der Landesregierung hat das Unabhängige Landeszentrum für Datenschutz Gutachten zu erstellen und Berichte zu erstatten. Es legt dem Landtag jährlich einen Tätigkeitsbericht vor.

(6) Für die Erfüllung der Aufgaben ist die notwendige Personal- und Sachausstattung zur Verfügung zu stellen; die Mittel sind im Einzelplan des Landtages in einem gesonderten Kapitel auszuweisen.

§ 40

Anrufung des Unabhängigen Landeszentrums für Datenschutz

Jede oder jeder hat das Recht, sich unmittelbar an das Unabhängige Landeszentrum für Datenschutz zu wenden, wenn sie oder er annimmt, dass bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen datenschutzrechtliche Vorschriften verletzt wurden. Dies gilt auch für Beschäftigte der öffentlichen Stellen, ohne dass der Dienstweg einzuhalten ist.

§ 41

Kontrollaufgaben

(1) Die öffentlichen Stellen sind verpflichtet, das Unabhängige Landeszentrum für Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist dabei insbesondere

1. Auskunft zu erteilen sowie Einsicht in Unterlagen und Dateien zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen; besondere Amts- und Berufsgeheimnisse stehen dem nicht entgegen;

2. Zutritt zu Diensträumen zu gewähren.

Das Unabhängige Landeszentrum für Datenschutz darf im Rahmen von Kontrollen personenbezogene Daten auch ohne Kenntnis der Betroffenen erheben. Die Benachrichtigung der Betroffenen richtet sich nach § 42 Abs. 4.

(2) Stellt die jeweils zuständige oberste Landesbehörde im Einzelfall fest, dass durch eine mit der Einsicht verbundene Bekanntgabe personenbezogener Daten die Sicherheit des Bundes oder eines Landes gefährdet wird, dürfen die Rechte nach Absatz 1 nur von der oder dem Landesbeauftragten für Datenschutz persönlich oder den von ihr oder ihm schriftlich besonders damit betrauten Beauftragten ausgeübt werden.

§ 42

Beanstandungen

(1) Stellt das Unabhängige Landeszentrum für Datenschutz Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzbestimmungen oder sonstige Mängel bei der Verarbeitung personenbezogener Daten bei öffentlichen Stellen fest, so fordert es diese zur Mängelbeseitigung auf.

(2) Bei erheblichen Verstößen oder sonstigen erheblichen Mängeln spricht das Unabhängige Landeszentrum für Datenschutz gegenüber der öffentlichen Stelle eine Beanstandung aus. Es soll zuvor die öffentliche Stelle zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auffordern und die zuständige Aufsichtsbehörde über die Beanstandung unterrichten.

(3) Mit der Feststellung von Mängeln und der Beanstandung sollen Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbunden werden.

(4) Die Betroffenen können mit Kenntnis der datenverarbeitenden Stelle nach pflichtgemäßem Ermessen von Verstößen gegen die Vorschriften dieses Gesetzes oder andere Datenschutzvorschriften unterrichtet werden.

§ 43

Serviceaufgaben

(1) Das Unabhängige Landeszentrum für Datenschutz berät und informiert die Bürgerinnen und Bürger über alle Fragen des Datenschutzes und der Datensicherheit, insbesondere über die ihnen bei der Verarbeitung ihrer Daten zustehenden Rechte sowie über geeignete technische Maßnahmen zum Selbstdatenschutz.

(2) Öffentliche Stellen können ihr Datenschutzkonzept durch das Unabhängige Landeszentrum für Datenschutz prüfen und beurteilen lassen.

(3) Das Unabhängige Landeszentrum für Datenschutz führt Fortbildungsveranstaltungen zu den Themen Datenschutz und Datensicherheit durch. Es berät nichtöffentliche Stellen auf Anfrage in Fragen von Datenschutz und Datensicherheit.

(4) Das Unabhängige Landeszentrum für Datenschutz kann für die Wahrnehmung der Aufgaben nach den Absätzen 1 bis 3 Entgelte erheben.

Abschnitt VII

Schlussvorschriften

§ 44

Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen den Vorschriften dieses Gesetzes personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, zweckwidrig verarbeitet, verändert, übermittelt, zum Abruf bereithält oder löscht,

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

Ordnungswidrig handelt auch, wer anonymisierte oder pseudonymisierte Daten mit anderen Informationen zusammenführt und dadurch die Betroffene oder den Betroffenen wieder bestimmbar macht oder wer sich bei pseudonymisierten Daten entgegen den Vorschriften dieses Gesetzes Zugriff auf die Zuordnungsfunktion verschafft.

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

§ 45

Aufgabenübergang

(1) Die am 30. Juni 2000 dem bei dem Präsidenten des Schleswig-Holsteinischen Landtages eingerichteten Landesbeauftragten für den Datenschutz sowie der Datenschutzaufsichtsbehörde im Innenministerium obliegenden Aufgaben gehen am 1. Juli 2000 auf die Anstalt über.

(2) Die Dienststelle im Sinne des Mitbestimmungsgesetzes Schleswig-Holstein (MBG Schl.-H.) "Landesbeauftragter für den Datenschutz bei dem Präsidenten des Schleswig-Holsteinischen Landtages" wird aufgelöst.

§ 46

Personalübergang

(1) Mit Wirkung vom 1. Juli 2000 gehen die Arbeits- und Ausbildungsverhältnisse der am 30. Juni 2000 beim Landesbeauftragten für den Datenschutz tätigen Arbeitnehmerinnen und Arbeitnehmer sowie der zu ihrer Ausbildung Beschäftigten vom Land Schleswig-Holstein auf das Unabhängige Landeszentrum für Datenschutz über.

(2) Für die Beschäftigten nach Absatz 1 gelten die bis zum Zeitpunkt der Errichtung der Anstalt maßgeblichen arbeitsvertraglichen Vereinbarungen und Tarifverträge in der jeweils geltenden Fassung weiter. Es gelten ferner die diese Tarifverträge künftig ändernden und ergänzenden Tarifverträge. Das Recht des Unabhängigen Landeszentrums für Datenschutz, für seine Beschäftigen Tarifverträge abzuschließen, bleibt hiervon unberührt. Bis zum Inkrafttreten neuer Tarifverträge sind für die ab 1. Juli 2000 eingestellten Arbeitnehmerinnen und Arbeitnehmer sowie zu ihrer Ausbildung Beschäftigen die nach Satz 1 und 2 maßgeblichen Tarifverträge anzuwenden.

(3) Für die Beschäftigen nach Absatz 1 werden die beim Land Schleswig-Holstein in einem Arbeits- oder Ausbildungsverhältnis zurückgelegten Zeiten einer Beschäftigung so angerechnet, wie wenn sie bei dem Unabhängigen Landeszentrum für Datenschutz zurückgelegt worden wären.

(4) Zur Sicherung der Ansprüche auf eine zusätzliche Alters- und Hinterbliebenenversorgung der Beschäftigten stellt die Anstalt sicher, dass die nach der Satzung der Versorgungsanstalt des Bundes und der Länder für eine Beteiligungsvereinbarung geforderten tatsächlichen und rechtlichen Voraussetzungen geschaffen werden.

(5) Die Beamtinnen und Beamten des Landes Schleswig-Holstein, die am 30. Juni 2000 beim Landesbeauftragten für den Datenschutz ihren Dienst ausgeübt haben, werden mit Wirkung vom 1. Juli 2000 nach § 36 Abs. 4 in Verbindung mit Abs. 3 des Landesbeamtengesetzes in den Dienst des Unabhängigen Landeszentrums für Datenschutz nach § 32 übernommen.

§ 47

Übergangsregelungen

(1) Der bisherige Landesbeauftragte für den Datenschutz wird bis zum Ablauf seiner Wahlzeit im Jahre 2004 Landesbeauftragter für Datenschutz nach diesem Gesetz. Eine erneute Wiederwahl ist ausgeschlossen.

(2) Der beim Landesbeauftragten für den Datenschutz gewählte Personalrat bleibt vorbehaltlich der §§ 20 und 21 MBG Schl.-H. über den 30. Juni 2000 bis zum Ablauf seiner regelmäßigen Amtszeit nach § 19 Abs. 1 MBG Schl.-H. bestehen. Die bis zum Ablauf des 30. Juni 2000 abgeschlossenen

Dienstvereinbarungen und Vereinbarungen nach § 59 MBG Schl.-H. gelten ab 1. Juli 2000 bis zum Abschluss neuer Dienstvereinbarungen in dem Unabhängigen Landeszentrum für Datenschutz fort.

(3) Die beim Landesbeauftragten für den Datenschutz bestellte Gleichstellungsbeauftragte und gewählte Schwerbehindertenvertretung bleiben über den 30. Juni 2000 hinaus bis zur Neubestellung oder Neuwahl im Amt. Die Gleichstellungsbeauftragte der Anstalt ist unverzüglich, spätestens bis zum 31. Juli 2000, zu bestellen.

(4) Soweit in diesem Gesetz Beträge in Euro genannt werden, gelten diese bis zum 31. Dezember 2001 auch als Beträge in DM; der Umrechnungskurs beträgt 1 Euro = 1,95583 DM.

§ 48

Inkrafttreten, Außerkrafttreten

(1) Dieses Gesetz tritt am 1. Juli 2000 in Kraft.

(2) Gleichzeitig treten

1. das Landesdatenschutzgesetz vom 30. Oktober 1991 (GVOBl. Schl.-H. S. 555), zuletzt geändert durch Gesetz vom 25. November 1999 (GVOBl. Schl.-H. S. 414),

2. das Gesetz zur Errichtung des Unabhängigen Landeszentrums für Datenschutz vom 25. November 1999 (GVOBl. Schl.-H. S. 414) und

3. die Landesverordnung über die zuständige Aufsichtsbehörde nach dem Bundesdatenschutzgesetz vom 8. Dezember 1992 (GVOBl. Schl.-H. S 533), geändert gemäß Verordnung vom 24. Oktober 1996 (GVOBl. Schl.-H. S. 652), außer Kraft.