juris

Gesamtes Gesetz

Amtliche Abkürzung:	LDSG	**Quelle:**	
Ausfertigungsdatum:	08.05.2018		
Gültig ab:	25.05.2018	**Fundstelle:**	GVBl. 2018, 93
Dokumenttyp:	Gesetz	**Gliederungs-Nr:**	204-1

Landesdatenschutzgesetz (LDSG) Vom 8. Mai 2018

Zum 10.01.2019 aktuellste verfügbare Fassung der Gesamtausgabe

Inhaltsübersicht

Abschnitt 4
Landesbeauftragte oder Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Abschnitt 5
Rechte der betroffenen Person

Abschnitt 6
Pflichten der Verantwortlichen und Auftragsverarbeiter

Der Landtag Rheinland-Pfalz hat das folgende Gesetz beschlossen:

Teil 1
Allgemeine Bestimmungen

§ 1
Zweck

(1) Zweck dieses Gesetzes ist es, ergänzende Regelungen zur Durchführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung - ABl. EU Nr. L 119 S. 1 -) in der jeweils geltenden Fassung zu treffen.

(2) Dieses Gesetz dient neben den zur Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. EU Nr. 119 S. 89) in der jeweils geltenden Fassung erlassenen Rechtsvorschriften auch der Umsetzung dieser Richtlinie.

§ 2
Anwendungsbereich

(1) Dieses Gesetz gilt für

1. die Behörden,

2. die Organe der Rechtspflege,

3. die Einrichtungen und sonstigen öffentlichen Stellen des Landes,

4. die kommunalen Gebietskörperschaften,

5. die sonstigen der Aufsicht des Landes oder der kommunalen Gebietskörperschaften unterstehenden juristischen Personen des öffentlichen Rechts und

6. die Vereinigungen der vorgenannten Stellen ungeachtet ihrer Rechtsform

(öffentliche Stellen), soweit diese personenbezogene Daten verarbeiten. Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts der in Satz 1 genannten öffentlichen Stellen, soweit diesen die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht, ungeachtet der Beteiligung nicht-öffentlicher Stellen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben einer öffentlichen Stelle des Landes wahr, ist sie insoweit öffentliche Stelle im Sinne des Gesetzes.

(2) Für Gerichte und Staatsanwaltschaften sowie für die Polizeibehörden und Ordnungsbehörden gilt Teil 2 dieses Gesetzes nur, soweit sie personenbezogene Daten zu anderen als den in § 26 Abs. 1 genannten Zwecken verarbeiten; im Übrigen gilt Teil 3 dieses Gesetzes.

(3) Der Landtag, seine Gremien, seine Mitglieder, die Fraktionen sowie deren Verwaltungen und deren Beschäftigte unterliegen nicht den Bestimmungen dieses Gesetzes, soweit sie in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeiten. Der Landtag erlässt insoweit unter Berücksichtigung seiner verfassungsrechtlichen Stellung, der Datenschutz-Grundverordnung und der Grundsätze dieses Gesetzes eine Datenschutzordnung.

(4) Soweit öffentliche Stellen als Unternehmen am Wettbewerb teilnehmen, sind auf diese § 20 und, unbeschadet anderer Rechtsgrundlagen, die Vorschriften des Bundesdatenschutzgesetzes (BDSG) für nicht-öffentliche Stellen anzuwenden.

(5) Auf öffentlich-rechtliche Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten sowie deren Vereinigungen finden § 26 BDSG und im Übrigen die Vorschriften des Bundesdatenschutzgesetzes über nicht-öffentliche Stellen Anwendung. Die Aufgaben der Aufsichtsbehörde werden von der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit wahrgenommen.

(6) Für die Verarbeitung personenbezogener Daten beim Südwestrundfunk (SWR) sowie beim Zweiten Deutschen Fernsehen (ZDF) finden die Bestimmungen dieses Gesetzes keine Anwendung. Dies gilt nicht für die Aufsicht über Hilfsunternehmen sowie Unternehmen, an denen der SWR oder das ZDF weder unmittelbar noch mittelbar, auch nicht zusammen mit anderen Anstalten oder Körperschaften des öffentlichen Rechts, mit Mehrheit beteiligt sind.

(7) Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(8) Die Bestimmungen dieses Gesetzes gehen denen des Landesverwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(9) Soweit besondere Rechtsvorschriften über den Datenschutz oder über Verfahren der Rechtspflege auf personenbezogene Daten anzuwenden sind, gehen diese den Bestimmungen dieses Gesetzes vor.

Teil 2
Verarbeitung personenbezogener Daten nach Maßgabe der Datenschutz-Grundverordnung

Abschnitt 1
Grundsätze der Verarbeitung personenbezogener Daten

§ 3
Zulässigkeit

Unbeschadet anderer Rechtsgrundlagen ist die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle zulässig, wenn sie zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

§ 4
Erhebung bei Dritten

Werden personenbezogene Daten bei einer dritten Person oder einer Stelle außerhalb des öffentlichen Bereichs erhoben, so ist diese auf Verlangen auf den Erhebungszweck hinzuweisen, soweit dadurch schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden. Werden die Daten aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, so ist auf die Auskunftspflicht, im Übrigen auf die Freiwilligkeit der Angaben hinzuweisen.

§ 5
Übermittlung an öffentliche Stellen

(1) Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde Stelle. Erfolgt die Übermittlung aufgrund eines Ersuchens einer öffentlichen Stelle, trägt diese

die Verantwortung. Die übermittelnde Stelle hat dann lediglich zu prüfen, ob sich das Übermittlungsersuchen im Rahmen der Aufgaben der ersuchenden Stelle hält. Die Rechtmäßigkeit des Ersuchens prüft sie nur, wenn im Einzelfall hierzu Anlass besteht; die ersuchende Stelle hat in dem Ersuchen der übermittelnden Stelle die für diese Prüfung erforderlichen Angaben zu machen. Erfolgt die Übermittlung durch automatisierten Abruf, so trägt die Verantwortung für die Rechtmäßigkeit des Abrufs die empfangende Stelle.

(2) Sind mit personenbezogenen Daten weitere personenbezogene Daten der betroffenen Person oder Dritter so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten an öffentliche Stellen zulässig, soweit nicht berechtigte Interessen der betroffenen Person oder Dritter an deren Geheimhaltung entgegenstehen; eine weitere Verarbeitung dieser Daten ist unzulässig.

§ 6
Löschung

Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem öffentlichen Archiv zur Übernahme anzubieten, ist eine Löschung personenbezogener Daten erst zulässig, nachdem die Unterlagen dem öffentlichen Archiv angeboten worden sind und von diesem die Feststellung erfolgt ist, dass es sich nicht um Archivgut handelt.

§ 7
Verarbeitung zu anderen Zwecken

(1) Eine Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, ist zulässig, wenn

1. es zur Abwehr einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder von erheblichen Nachteilen für das Gemeinwohl erforderlich ist,

2. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,

3. es erforderlich ist, Angaben der betroffenen Person zu überprüfen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

4. sich bei der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheint,

5. es zur Entscheidung über die Verleihung staatlicher Orden oder Ehrenzeichen oder von sonstigen staatlichen Ehrungen erforderlich ist oder

6.

sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, zur Rechnungsprüfung und zur Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; das gilt auch für die Verarbeitung personenbezogener Daten zu Aus- und Fortbildungszwecken durch den Verantwortlichen, soweit nicht berechtigte Interessen der betroffenen Person an der Geheimhaltung der Daten entgegenstehen.

(2) Eine Information der betroffenen Person über die Datenverarbeitung nach Absatz 1 erfolgt nicht, soweit und solange hierdurch der Zweck der Verarbeitung gefährdet würde.

(3) Ferner ist eine Zweckänderung zulässig, wenn

1. die Einholung der Einwilligung der betroffenen Person nicht möglich ist oder mit unverhältnismäßig hohem Aufwand verbunden wäre, aber offensichtlich ist, dass die Datenverarbeitung zu ihrem Schutz erfolgt und sie in Kenntnis des anderen Zwecks ihre Einwilligung erteilen würde oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die datenverarbeitende Stelle sie veröffentlichen dürfte, soweit nicht schutzwürdige Interessen der betroffenen Person offensichtlich entgegenstehen.

(4) Unterliegen die personenbezogenen Daten einem Berufsgeheimnis oder einem besonderen Amtsgeheimnis und sind sie der datenverarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, finden die Absätze 1 und 3 keine Anwendung.

(5) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen für andere Zwecke nur insoweit verarbeitet werden, als dies zur Abwehr erheblicher Gefahren für die öffentliche Sicherheit, insbesondere für Leben, Gesundheit oder Freiheit, erforderlich ist.

§ 8
Datengeheimnis

(1) Den bei dem Verantwortlichen oder in dessen Auftrag beschäftigten Personen, die dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, diese Daten zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder unbefugt zu offenbaren (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

(2) Die in Absatz 1 Satz 1 genannten Personen sind bei der Aufnahme ihrer Tätigkeit über ihre Pflichten nach Absatz 1 sowie die sonstigen bei ihrer

Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten und auf deren Einhaltung zu verpflichten.

§ 9
Datenschutz-Folgenabschätzung

(1) Eine Datenschutz-Folgenabschätzung gemäß Artikel 35 der Datenschutz-Grundverordnung durch den Verantwortlichen kann unterbleiben, soweit

1. eine solche für den Verarbeitungsvorgang bereits vom fachlich zuständigen Ministerium oder einer von diesem ermächtigten öffentlichen Stelle durchgeführt wurde und dieser Verarbeitungsvorgang im Wesentlichen unverändert übernommen wird oder

2. der konkrete Verarbeitungsvorgang in einer Rechtsvorschrift geregelt ist und im Rechtsetzungsverfahren bereits eine Datenschutz-Folgenabschätzung erfolgt ist, es sei denn, dass in der Rechtsvorschrift etwas anderes bestimmt ist.

Die Ministerien stellen den öffentlichen Stellen die Ergebnisse der von ihnen und der von ihnen ermächtigten öffentlichen Stellen durchgeführten Datenschutz-Folgenabschätzungen zur Verfügung.

(2) Entwickelt eine öffentliche Stelle ein automatisiertes Verfahren, das zum Einsatz durch öffentliche Stellen bestimmt ist, so kann sie, sofern die Voraussetzungen des Artikels 35 Abs. 1 der Datenschutz-Grundverordnung bei diesem Verfahren vorliegen, die Datenschutz-Folgenabschätzung nach den Artikeln 35 und 36 der Datenschutz-Grundverordnung durchführen. Soweit das Verfahren von öffentlichen Stellen im Wesentlichen unverändert übernommen wird, kann eine weitere Datenschutz-Folgenabschätzung durch die übernehmenden öffentlichen Stellen unterbleiben.

§ 10
Entsprechende Anwendung der Datenschutz-Grundverordnung

Fällt die Verarbeitung personenbezogener Daten nicht in den Anwendungsbereich der Datenschutz-Grundverordnung, sind ihre Bestimmungen entsprechend anzuwenden, es sei denn, dieses Gesetz oder andere Rechtsvorschriften enthalten spezielle Regelungen.

Abschnitt 2
Rechte der betroffenen Person

§ 11
Beschränkung der Informationspflicht nach den Artikeln 13 und 14 der Datenschutz-Grundverordnung

(1) Der Verantwortliche kann von der Erteilung der Information über personenbezogene Daten absehen, soweit und solange

1.

die Information die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

2. dies zur Verfolgung von Straftaten und Ordnungswidrigkeiten erforderlich ist oder

3. die Information dazu führen würde, dass Sachverhalte aufgedeckt werden, die aufgrund einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind.

Die Gründe für ein Absehen von der Information sind zu dokumentieren. Die Information ist nachzuholen, wenn die Gründe nach Satz 1 nicht mehr bestehen. Die betroffene Person ist über die Beschränkung der Informationspflicht zu informieren, soweit dies nicht dem Zweck der Beschränkung abträglich ist.

(2) Der Rechnungshof Rheinland-Pfalz kann von der Erteilung der Information absehen, soweit und solange hierdurch der Zweck oder die Durchführung der Prüfungstätigkeit des Rechnungshofs gefährdet oder wesentlich erschwert würde. Absatz 1 Satz 2 bis 4 gilt entsprechend.

§ 12
Auskunftsrecht der betroffenen Person nach Artikel 15 der Datenschutz-Grundverordnung

(1) Bezieht sich eine nach Artikel 15 der Datenschutz-Grundverordnung verlangte Auskunft auf personenbezogene Daten, die an

1. eine Behörde der Staatsanwaltschaft, eine Polizeidienststelle oder eine andere zur Verfolgung von Straftaten zuständige Stelle,

2. eine Verfassungsschutzbehörde, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst oder

3. das Bundesministerium der Verteidigung oder eine Behörde seines nachgeordneten Bereichs

übermittelt wurden, so ist mit dieser Behörde vor der Erteilung der Auskunft das Einvernehmen herzustellen. Im Falle des Satzes 1 Nr. 3 ist dies nur erforderlich, wenn die Erteilung der Auskunft die Sicherheit des Bundes berühren könnte. Die Sätze 1 und 2 gelten entsprechend für personenbezogene Daten, die von einer Behörde nach Satz 1 übermittelt wurden.

(2) Der Verantwortliche kann die Erteilung einer Auskunft ablehnen, soweit und solange

1. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

2. die Auskunft die Verfolgung von Straftaten oder Ordnungswidrigkeiten gefährden würde oder

3. die Auskunft dazu führen würde, dass Sachverhalte, die aufgrund einer Rechtsvorschrift oder wegen der Rechte und Freiheiten einer anderen Person geheim zu halten sind, aufgedeckt werden.

Abgelehnt werden kann auch eine Auskunft über personenbezogene Daten, die ausschließlich zu Zwecken der Gewährleistung der Datensicherheit oder der Datenschutzkontrolle verarbeitet werden und durch geeignete technische und organisatorische Maßnahmen gegen eine Verarbeitung zu anderen Zwecken geschützt sind, wenn die Erteilung der Auskunft einen unverhältnismäßigen Aufwand erfordern würde.

(3) Die Ablehnung der Auskunft ist zu begründen, soweit nicht durch die Mitteilung der Gründe der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Soweit die Ablehnung der Auskunft nicht nach Satz 1 begründet wird, sind die Gründe dafür aktenkundig zu machen. Die betroffene Person ist darauf hinzuweisen, dass sie sich an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

(4) Wird der betroffenen Person eine Auskunft nicht erteilt, so ist die Auskunft auf Verlangen der betroffenen Person der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, es sei denn, dass die zuständige oberste Landesbehörde im Einzelfall feststellt, dass durch die Auskunft die Sicherheit des Bundes oder eines Landes gefährdet würde. Wird der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit eine Auskunft nicht erteilt, so sind die Gründe dafür aktenkundig zu machen. Die Mitteilung der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt.

§ 13
Beschränkung der Benachrichtigung nach Artikel 34 der Datenschutz-Grundverordnung

Der Verantwortliche kann von der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person absehen, soweit und solange die Benachrichtigung

1. die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

2. die Benachrichtigung die Verfolgung von Straftaten oder Ordnungswidrigkeiten gefährden würde,

3.

dazu führen würde, dass Sachverhalte, die nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind, aufgedeckt werden, oder

4. die Funktionsfähigkeit von Datenverarbeitungssystemen einer öffentlichen Stelle gefährden würde.

Abschnitt 3
Landesbeauftragte oder Landesbeauftragter für den Datenschutz und die Informationsfreiheit

§ 14
Rechtsstellung

(1) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit steht in einem öffentlich-rechtlichen Amtsverhältnis und ist in Ausübung ihres oder seines Amtes unabhängig und nur dem Gesetz unterworfen. Sie oder er untersteht der Dienstaufsicht der Präsidentin oder des Präsidenten des Landtags, soweit nicht ihre oder seine Unabhängigkeit beeinträchtigt wird.

(2) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit soll neben der erforderlichen Erfahrung und Sachkunde nach Artikel 53 Abs. 2 der Datenschutz-Grundverordnung, insbesondere im Bereich des Schutzes personenbezogener Daten, die Befähigung zum Richteramt oder für das vierte Einstiegsamt haben. Der Landtag wählt die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit in geheimer Wahl mit der Mehrheit seiner Mitglieder auf Vorschlag einer Fraktion; eine Aussprache findet nicht statt. Sie oder er wird nach der Wahl durch den Landtag auf die Dauer von acht Jahren in ein öffentlich-rechtliches Amtsverhältnis berufen. Die Wiederwahl und die Berufung für eine weitere Amtszeit sind zulässig. Das Amt ist im Übrigen bis zum Eintritt der Nachfolge weiterzuführen.

(3) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit kann außer im Falle der Amtsenthebung nach Artikel 53 Abs. 4 der Datenschutz-Grundverordnung nur auf Antrag entlassen werden. Für die Amtsenthebung ist der Landtag zuständig. Das Verfahren der Amtsenthebung richtet sich nach der vom Landtag erlassenen Datenschutzordnung nach § 2 Abs. 3 Satz 2.

(4) Die Vergütung der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit ist durch Vertrag zu regeln. Das Amt kann auch einer beurlaubten Beamtin oder einem beurlaubten Beamten oder einer Beamtin oder einem Beamten im Ruhestand übertragen werden.

(5) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist, auch nach Beendigung des Amtsverhältnisses, verpflichtet, über amtlich bekannt gewordene Angelegenheiten Verschwiegenheit zu wahren. Dies gilt nicht für Mitteilungen im dienstlichen

Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

(6) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit bestellt eine Stellvertreterin oder einen Stellvertreter für die Führung der Geschäfte im Falle ihrer oder seiner Verhinderung.

(7) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit kann an den Sitzungen des Landtags und seiner Ausschüsse nach Maßgabe der Geschäftsordnung des Landtags teilnehmen. Der Landtag und seine Ausschüsse können ihre oder seine Anwesenheit verlangen. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit kann sich in Ausschusssitzungen zu Fragen äußern, die für den Datenschutz von Bedeutung sind.

§ 15
Zuständigkeit und Organisation

(1) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist Aufsichtsbehörde im Sinne des Artikels 51 der Datenschutz-Grundverordnung, soweit der Anwendungsbereich dieses Gesetzes eröffnet ist.

(2) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist ferner Aufsichtsbehörde im Sinne des § 40 BDSG für die Kontrolle der Durchführung des Datenschutzes bei der Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen.

(3) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit darf neben ihrem oder seinem Amt kein anderes besoldetes Amt und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. In Ergänzung zu der Regelung in Artikel 52 Abs. 3 der Datenschutz-Grundverordnung hat die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit auch für die Dauer von fünf Jahren nach ihrer oder seiner Amtszeit von allen mit den Aufgaben ihres früheren Amtes nicht zu vereinbarenden Handlungen und nicht zu vereinbarenden entgeltlichen oder unentgeltlichen Tätigkeiten abzusehen.

(4) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit wird bei der Präsidentin oder dem Präsidenten des Landtags eingerichtet und hat die Stellung einer obersten Landesbehörde mit Sitz in Mainz. Zur Erfüllung der Aufgaben ist die notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Die Mittel sind im Einzelplan des Landtags in einem gesonderten Kapitel auszuweisen.

(5) Das Personal untersteht der Dienstaufsicht der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit. Das Recht der Ernennung, Versetzung, Abordnung, Ruhestandsversetzung und Entlassung der Beamtinnen und Beamten des ersten, zweiten und dritten

Einstiegsamtes, unabhängig von ihrer besoldungsrechtlichen Einstufung, sowie des vierten Einstiegsamtes bis einschließlich der Besoldungsgruppe A 15 übt die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit aus. Für Beamtinnen und Beamte des vierten Einstiegsamtes ab der Besoldungsgruppe A 16 übt die Präsidentin oder der Präsident des Landtags dieses Recht auf Vorschlag und im Einvernehmen mit der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit aus. Beamtinnen und Beamte können nur im Einvernehmen mit der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit zu dieser oder diesem versetzt oder abgeordnet werden. Für die sonstigen Bediensteten gelten die Sätze 2 und 4 entsprechend.

§ 16
Aufgaben, Mitwirkungspflichten

(1) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit nimmt die Aufgaben nach den Artikeln 57 und 59 der Datenschutz-Grundverordnung wahr. Dabei kontrolliert sie oder er die Einhaltung der Vorschriften der Datenschutz-Grundverordnung, dieses Gesetzes und anderer datenschutzrechtlicher Bestimmungen.

(2) Die Aufsicht durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit erstreckt sich nicht auf die Mitglieder des Rechnungshofs Rheinland-Pfalz, soweit diese bei ihrer Prüfungs- und Beratungstätigkeit im Rahmen ihrer richterlichen Unabhängigkeit handeln.

(3) Die Landesregierung nimmt zu dem Tätigkeitsbericht der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit nach Artikel 59 der Datenschutz-Grundverordnung innerhalb von sechs Monaten gegenüber dem Landtag Stellung.

(4) Die öffentlichen Stellen sind verpflichtet, die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit bei der Erfüllung der Aufgaben zu unterstützen.

§ 17
Befugnisse nach Artikel 58 der Datenschutz-Grundverordnung

(1) Die Befugnisse der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit nach Artikel 58 der Datenschutz-Grundverordnung beziehen sich auf Verstöße gegen Bestimmungen der Datenschutz-Grundverordnung, dieses Gesetzes oder anderer Datenschutzbestimmungen. Die Befugnisse nach Artikel 58 der Datenschutz-Grundverordnung übt die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit

1. gegenüber den Verantwortlichen,

2. bei den Gemeinden, Gemeindeverbänden und Landkreisen und den sonstigen der Aufsicht des Landes oder der Gemeinden,

Gemeindeverbände und Landkreisen unterstehenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem vertretungsberechtigten Organ

aus. Zusätzlich zu den Befugnissen nach Artikel 58 der Datenschutz-Grundverordnung kann die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Verstöße gemäß Satz 1 beanstanden. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit kann von der öffentlichen Stelle eine Stellungnahme innerhalb einer angemessenen Frist fordern. In den Fällen des Satzes 2 Nr. 2 ist gleichzeitig auch die zuständige Aufsichtsbehörde zu unterrichten.

(2) Die Stellungnahme nach Absatz 1 Satz 4 soll auch die Maßnahmen darstellen, die die Verstöße beseitigen sollen. Die in Absatz 1 Satz 2 Nr. 2 genannten Stellen leiten der zuständigen Aufsichtsbehörde eine Abschrift ihrer Stellungnahme zu.

(3) Im Rahmen der Befugnisse der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit haben die öffentlichen Stellen Zugang zu den Diensträumen, einschließlich aller Datenverarbeitungsanlagen und -geräte sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer oder seiner Aufgaben notwendig sind, zu gewähren.

(4) Für die Kontrolle durch die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit hinsichtlich personenbezogener Daten, die einem Berufs- oder besonderem Amtsgeheimnis unterliegen, gilt § 29 Abs. 3 BDSG entsprechend.

(5) Die Befugnis, Geldbußen zu verhängen, richtet sich nach § 24. Für Amtshandlungen nach diesem Gesetz und nach der Datenschutz-Grundverordnung kann die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Kosten (Gebühren und Auslagen) erheben; § 24 Abs. 3 gilt entsprechend. Das für den Datenschutz zuständige Ministerium wird ermächtigt, im Benehmen mit der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit die Gebührentatbestände und Gebührensätze durch Rechtsverordnung zu bestimmen.

§ 18
Datenschutzkommission

(1) Bei der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit wird eine Datenschutzkommission gebildet, die aus acht Mitgliedern besteht. In die Datenschutzkommission entsenden der Landtag sieben Mitglieder und die Landesregierung ein Mitglied. Die vom Landtag zu entsendenden Mitglieder verteilen sich auf die Fraktionen nach dem d'Hondtschen Höchstzahlverfahren, jedoch stellt jede Fraktion mindestens ein Mitglied.

(2) Die Mitglieder der Datenschutzkommission werden vom Landtag aus seiner Mitte für die Dauer der Wahlperiode des Landtags, von der Landesregierung für die Dauer von fünf Jahren entsandt.

(3) Die Datenschutzkommission unterstützt die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit bei der Wahrnehmung ihrer oder seiner Aufgaben nach diesem Gesetz. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit nimmt an den Sitzungen der Datenschutzkommission teil. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit unterrichtet die Datenschutzkommission über Maßnahmen nach § 17. Der Tätigkeitsbericht der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit ist in der Datenschutzkommission eine angemessene Zeit vor Übermittlung an den Landtag und die Landesregierung zu beraten.

(4) Die Datenschutzkommission tritt auf Antrag eines ihrer Mitglieder oder der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit zusammen.

(5) Die Datenschutzkommission wählt aus dem Kreis der vom Landtag entsandten Mitglieder eine oder einen Vorsitzenden und eine Stellvertreterin oder einen Stellvertreter. Sie gibt sich eine Geschäftsordnung.

(6) Die Mitglieder der Datenschutzkommission sind verpflichtet, auch nach ihrem Ausscheiden über die ihnen bei ihrer amtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu wahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

(7) Die oder der Vorsitzende der Datenschutzkommission erhält eine monatliche Aufwandsentschädigung in gleicher Höhe wie die oder der Vorsitzende eines Ausschusses des Landtags.

(8) Die Mitglieder der Datenschutzkommission erhalten Reisekostenvergütung nach den Bestimmungen des Landesreisekostengesetzes.

Abschnitt 4
Besonderer Datenschutz

§ 19
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung ist auf der Basis einer ausdrücklichen Einwilligung der betroffenen Person zulässig. Die Einwilligung in die Verarbeitung genetischer oder biometrischer Daten oder Gesundheitsdaten bedarf der Schriftform. Die Übermittlung derartiger Daten auf der Grundlage einer Einwilligung ist nur wirksam, wenn die empfangende Stelle Kenntnis von Inhalt und Reichweite der Einwilligung hat.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Datenschutz-Grundverordnung durch öffentliche Stellen ist zulässig, wenn sie aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist und soweit die Interessen des Verantwortlichen an der Datenverarbeitung die schutzwürdigen Interessen der betroffenen Person überwiegen. Ein erhebliches öffentliches Interesse im Sinne des Satzes 1 ist insbesondere anzunehmen bei

1. der Abwehr einer Gefahr für die öffentliche Sicherheit,

2. der Verfolgung von Straftaten von Bedeutung,

3. der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen oder

4. der Abwehr von Nachteilen für das Gemeinwohl oder zur Wahrung von Belangen des Gemeinwohls.

(3) Bei der Verarbeitung genetischer oder biometrischer Daten oder Gesundheitsdaten haben die Verantwortlichen angemessene und spezifische Maßnahmen, insbesondere technische und organisatorische Maßnahmen, zur Wahrung der Grundrechte und Interessen der betroffenen Person vorzusehen. Mindestens haben die Verantwortlichen

1. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem die Daten eingegeben, verändert oder entfernt worden sind,

2. die an den Verarbeitungsvorgängen Beteiligten zu sensibilisieren,

3. den Zugang zu den Daten beim Verantwortlichen und von Auftragsverarbeitern zu beschränken,

4. die Grundsätze der Datenminimierung und Speicherbegrenzung sowie die Notwendigkeit einer Datenschutz-Folgenabschätzung zu berücksichtigen,

5. die Daten im Fall der Übermittlung zu verschlüsseln,

6. die Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung der Daten sicherzustellen,

7. die Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,

8. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzurichten und

9. im Fall einer Übermittlung oder Verarbeitung für andere Zwecke, die Einhaltung der Vorgaben dieses Gesetzes sowie der Datenschutz-Grundverordnung durch spezifische Verfahrensregelungen sicherzustellen.

Artikel 32 der Datenschutz-Grundverordnung bleibt unberührt.

(4) Die Verarbeitung von genetischen oder biometrischen Daten oder Gesundheitsdaten im Auftrag ist nur zulässig, wenn der Auftragsverarbeiter entsprechend dem Schutzbedarf der Daten angemessene Vorkehrungen zum Datenschutz im Sinne des Absatzes 3 getroffen hat und keine überwiegenden schutzwürdigen Interessen der betroffenen Person einer Auslagerung der Datenverarbeitung entgegenstehen. Die Beauftragung von Stellen außerhalb des Geltungsbereichs der Datenschutz-Grundverordnung ist unzulässig.

(5) Sofern an einer gemeinsamen Verarbeitung personenbezogener Daten im Sinne von Artikel 26 der Datenschutz-Grundverordnung, die zumindest auch genetische oder biometrische Daten oder Gesundheitsdaten umfasst, Stellen beteiligt sind, die dem Geltungsbereich dieses Gesetzes unterliegen, ist diese nur zulässig, wenn die Erfüllung der in der Datenschutz-Grundverordnung enthaltenen Anforderungen vor Beginn der Datenverarbeitung gegenüber der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit nachgewiesen worden ist.

§ 20
Datenverarbeitung bei Dienst- und Beschäftigungsverhältnissen

(1) Personenbezogene Daten von Bewerberinnen und Bewerbern für ein Dienst- oder Beschäftigungsverhältnis sowie personenbezogene Daten von Personen in einem Dienst- oder Beschäftigungsverhältnis dürfen nur verarbeitet werden, wenn dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Beschäftigungsverhältnisses oder zur Durchführung innerdienstlicher, planerischer, organisatorischer, personeller, sozialer oder haushalts- und kostenrechnerischer Maßnahmen, insbesondere zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder in einer Rechtsvorschrift, einem Tarifvertrag oder einer Dienst- oder Betriebsvereinbarung (Kollektivvereinbarung) vorgesehen ist. Eine Übermittlung der Daten von Personen in einem Dienst- oder Beschäftigungsverhältnis an Personen und Stellen außerhalb des öffentlichen Bereichs ist nur zulässig, wenn die Empfängerin oder der Empfänger ein rechtliches Interesse darlegt, der Dienstverkehr es erfordert oder die betroffene Person eingewilligt hat. Die Datenübermittlung an einen künftigen oder neuen Dienstherrn oder Arbeitgeber ist nur mit Einwilligung der betroffenen Person zulässig oder wenn es in einer Rechtsvorschrift vorgesehen ist.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Personen in einem Dienst- oder Beschäftigungsverhältnis auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Dienst- oder Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder der Dienstherr oder der Arbeitgeber und die beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Die beschäftigte Person ist über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Artikel 7 Abs. 3 der Datenschutz-Grundverordnung aufzuklären.

(3) Abweichend von Artikel 9 Abs. 1 der Datenschutz-Grundverordnung ist die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Dienst- und Beschäftigungsverhältnisses im Sinne des Absatzes 1 zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Beamtenrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes, der Gesundheitsvorsorge oder der Arbeitsmedizin erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Erfolgt die Verarbeitung auf der Grundlage einer Einwilligung, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

(4) Auf die Verarbeitung von Personalaktendaten der Beschäftigten sowie der Auszubildenden finden die für Beamtinnen und Beamte geltenden Bestimmungen des Beamtenstatusgesetzes und des Landesbeamtengesetzes entsprechend Anwendung, es sei denn, besondere Rechtsvorschriften oder tarifliche Vereinbarungen gehen vor.

(5) Die Speicherung, Veränderung oder Nutzung der bei medizinischen oder psychologischen Untersuchungen und Tests zum Zweck der Feststellung der Eignung erhobenen Daten ist nur zulässig, wenn dies für Zwecke der Eingehung oder Durchführung eines Dienst- oder Beschäftigungsverhältnisses erforderlich ist. Eine Verarbeitung dieser Daten zu anderen Zwecken ist nur mit Einwilligung der betroffenen Person zulässig. Die Beschäftigungsbehörde darf von der untersuchenden Ärztin oder dem untersuchenden Arzt nur die Übermittlung des Ergebnisses der Eignungsuntersuchung und dabei festgestellter Risikofaktoren verlangen. § 47 Abs. 2 des Landesbeamtengesetzes bleibt unberührt.

(6) Personenbezogene Daten, die vor der Eingehung eines Dienst- oder Beschäftigungsverhältnisses erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein Dienst- oder Beschäftigungsverhältnis nicht zustande kommt, es sei denn, dass die betroffene Person in die weitere Speicherung eingewilligt hat oder dies wegen eines bereits anhängigen oder wahrscheinlich zu erwartenden Rechtsstreits erforderlich ist. Nach Beendigung eines Dienst- oder Beschäftigungsverhältnisses sind

personenbezogene Daten zu löschen, wenn diese Daten nicht mehr benötigt werden, es sei denn, es stehen Rechtsvorschriften der Löschung entgegen.

(7) Soweit Daten der Personen in einem Dienst- oder Beschäftigungsverhältnis im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach Artikel 32 der Datenschutz-Grundverordnung gespeichert werden, dürfen sie nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

§ 21
Videoüberwachung

(1) Die Verarbeitung personenbezogener Daten mit Hilfe von optisch-elektronischen Einrichtungen (Videoüberwachung) ist zulässig, wenn dies

1. zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt,

2. zur Wahrnehmung des Hausrechts oder

3. sonst zum Schutz des Eigentums oder Besitzes oder zur Kontrolle von Zugangsberechtigungen

erforderlich ist und keine Anhaltspunkte bestehen, dass überwiegende schutzwürdige Interessen der betroffenen Personen entgegenstehen. Bei der Videoüberwachung von Fahrzeugen und öffentlich zugänglichen Einrichtungen des öffentlichen Schienen-, Schiffs-, Bus- und Seilbahnverkehrs gilt der Schutz von Leben, Gesundheit oder Freiheit von sich dort aufhaltenden Personen als ein besonders wichtiges Interesse.

(2) Der Umstand der Videoüberwachung, die Angaben nach Artikel 13 Abs. 1 Buchst. a bis c der Datenschutz-Grundverordnung sowie die Möglichkeit, beim Verantwortlichen die weiteren Informationen nach Artikel 13 der Datenschutz-Grundverordnung zu erhalten, sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Eine Verarbeitung zu anderen Zwecken ist nur zulässig, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich oder dies gesetzlich geregelt ist.

(4) Werden durch eine Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist die betroffene Person über eine Verarbeitung entsprechend Artikel 13 Abs. 1 der Datenschutz-Grundverordnung zu informieren, soweit und solange der Zweck der Verarbeitung hierdurch nicht gefährdet wird. § 12 gilt entsprechend.

(5) Das nach Absatz 1 gewonnene Bildmaterial und daraus gefertigte Unterlagen sind spätestens nach zwei Monaten zu löschen oder zu vernichten, soweit diese nicht zur Verfolgung von Straftaten, zur Geltendmachung von Rechtsansprüchen oder wegen entgegenstehender schutzwürdiger Interessen betroffener Personen, insbesondere zur Behebung

einer bestehenden Beweisnot, erforderlich sind. Bis zur Aussonderung der Daten ist die Verarbeitung der personenbezogenen Daten im Sinne von Artikel 18 der Datenschutz-Grundverordnung einzuschränken.

(6) Überwacht ein Verantwortlicher zur Wahrnehmung einer Aufgabe systematisch, dauerhaft oder in einem eine Vielzahl von Personen betreffenden Umfang öffentlich zugängliche Bereiche und besteht ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen, ist eine Datenschutz-Folgenabschätzung nach Artikel 35 Abs. 3 Buchst. c der Datenschutz-Grundverordnung durchzuführen.

(7) Der Einsatz von Attrappen ist unter den Voraussetzungen der Absätze 1 und 2 zulässig.

§ 22
Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Der wissenschaftliche und historische Forschung betreibende Verantwortliche darf personenbezogene Daten im Sinne von Artikel 9 Abs. 1 der Datenschutz-Grundverordnung auch ohne Einwilligung der betroffenen Person für wissenschaftliche und historische Forschungszwecke verarbeiten, wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(2) Für Zwecke der wissenschaftlichen oder historischen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nach Maßgabe des Absatzes 1 für weitere, mit dem ursprünglichen Zweck vereinbare Zwecke der Forschung verarbeitet werden.

(3) Eine wirksame Einwilligung der betroffenen Person zur Verarbeitung von genetischen oder biometrischen Daten oder Gesundheitsdaten bedarf der Schriftform.

(4) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Es muss sichergestellt sein, dass die Merkmale, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können, von einer Stelle verwaltet werden, die räumlich, organisatorisch und personell getrennt von der forschenden Stelle ist, wenn dem nicht zwingende wissenschaftliche Gründe entgegenstehen. Die Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(5) Der wissenschaftliche und historische Forschung betreibende Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn

1. die betroffene Person eingewilligt hat oder

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

(6) Die Absätze 1 bis 5 gelten entsprechend für die Datenverarbeitung zu statistischen Zwecken.

§ 23
Verarbeitung zu Zwecken der parlamentarischen Kontrolle

Die Landesregierung darf personenbezogene Daten einschließlich Daten im Sinne von Artikel 9 Abs. 1 der Datenschutz-Grundverordnung zur Beantwortung parlamentarischer Anfragen sowie zur Vorlage von Unterlagen und Berichten an den Landtag in dem dafür erforderlichen Umfang verarbeiten. Eine Übermittlung der personenbezogenen Daten zu einem der in Satz 1 genannten Zwecke ist nicht zulässig, wenn dies wegen des streng persönlichen Charakters der Daten für die betroffene Person unzumutbar ist oder wenn der Eingriff in ihr informationelles Selbstbestimmungsrecht unverhältnismäßig ist. Satz 2 gilt nicht, wenn durch die Datenschutzordnung im Sinne des § 2 Abs. 3 Satz 2 oder sonstige geeignete Maßnahmen sichergestellt ist, dass schutzwürdige Interessen der betroffenen Person nicht beeinträchtigt werden. Besondere gesetzliche Übermittlungsverbote bleiben unberührt.

Abschnitt 5
Ordnungswidrigkeiten und Strafbestimmungen

§ 24
Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer entgegen den Bestimmungen der Datenschutz-Grundverordnung, dieses Gesetzes oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten, personenbezogene Daten, die nicht offenkundig sind,

1. erhebt, speichert, unbefugt verwendet, verändert, übermittelt, weitergibt, zum Abruf bereithält, den Personenbezug herstellt oder löscht oder

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

Ordnungswidrig handelt auch, wer unter den in Satz 1 genannten Voraussetzungen Einzelangaben über persönliche oder sachliche Verhältnisse einer nicht mehr bestimmbaren Person mit anderen Informationen zusammenführt und dadurch die betroffene Person wieder bestimmbar macht.

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

(3) Gegen öffentliche Stellen werden keine Geldbußen verhängt. Dies gilt nicht für öffentliche Stellen nach § 2 Abs. 4, soweit die Verarbeitung im Rahmen einer Tätigkeit erfolgt, hinsichtlich derer die öffentliche Stelle mit anderen Verarbeitern im Wettbewerb steht.

§ 25
Strafbestimmung

(1) Wer gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, eine der in § 24 Abs. 1 genannten Handlungen begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt.

(3) Antragsberechtigt sind die betroffene Person, der Verantwortliche, der Auftragsverarbeiter und die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit.

Teil 3
Verarbeitung personenbezogener Daten nach Maßgabe der Richtlinie (EU) 2016/680

Abschnitt 1
Anwendungsbereich, Begriffsbestimmungen

§ 26
Anwendungsbereich

(1) Die Bestimmungen dieses Teils gelten für Gerichte und Staatsanwaltschaften sowie für die Polizeibehörden und Ordnungsbehörden, soweit diese personenbezogene Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, verarbeiten. Die in Satz 1 benannten Stellen gelten dabei als Verantwortliche. Soweit dieser Teil Bestimmungen für Auftragsverarbeiter enthält, gilt er auch für diese.

(2) Als eine Verarbeitung personenbezogener Daten im Sinne des Absatzes 1 gilt die ganz oder teilweise automatisierte oder nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

§ 27
Begriffsbestimmungen

Es bezeichnen die Begriffe:

1. „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person)

beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann;

2. „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung" die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling" jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben, der Interessen, der Zuverlässigkeit, des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können;

6. „Dateisystem" jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. „zuständige Behörde"

   a) eine staatliche Stelle, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten oder die Strafvollstreckung, einschließlich

des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig ist, oder

b) eine andere Stelle oder Einrichtung, der durch eine Rechtsvorschrift die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, übertragen wurde;

8. „Verantwortlicher" die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

9. „Auftragsverarbeiter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

10. „Empfänger" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht; Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

11. „Verletzung des Schutzes personenbezogener Daten" eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten, die verarbeitet wurden, geführt hat;

12. „genetische Daten" personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der betreffenden Person gewonnen wurden;

13. „biometrische Daten" mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten;

14. „Gesundheitsdaten" personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

15. „besondere Kategorien personenbezogener Daten"

    a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,

    b) genetische Daten,

    c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

    d) Gesundheitsdaten und

    e) Daten zum Sexualleben oder zur sexuellen Orientierung;

16. „Aufsichtsbehörde" eine von einem Mitgliedsstaat gemäß Artikel 41 der Richtlinie (EU) 2016/680 eingerichtete unabhängige staatliche Stelle;

17. „internationale Organisation" eine völkerrechtliche Organisation und ihre nachgeordneten Stellen sowie jede sonstige Einrichtung, die durch eine von zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde;

18. „Einwilligung" jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden Daten einverstanden ist.

Abschnitt 2
Rechtsgrundlagen der Verarbeitung personenbezogener Daten

§ 28
Allgemeine Grundsätze

(1) Die Verarbeitung personenbezogener Daten durch eine nach § 26 Abs. 1 zuständige Stelle zu den dort genannten Zwecken ist zulässig, wenn und soweit sie zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist.

(2) Personenbezogene Daten

1. müssen auf rechtmäßige Weise verarbeitet werden,

2. müssen für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,

3. müssen dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet sind, nicht übermäßig sein,

4. müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,

5. dürfen nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht, und

6. müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Maßnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

§ 29
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist, geeignete Garantien für die Rechtsgüter der betroffenen Personen bestehen und

1. wenn sie nach geltendem Recht zulässig ist oder

2. die Verarbeitung der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dient oder

3. wenn sie sich auf Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.

(2) Geeignete Garantien im Sinne des Absatzes 1 können insbesondere sein

1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle,

2. die Festlegung von besonderen Aussonderungsprüffristen,

3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,

4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb des Verantwortlichen,

5. die von anderen Daten getrennte Verarbeitung,

6. die Pseudonymisierung personenbezogener Daten,

7. die Verschlüsselung personenbezogener Daten oder

8. spezifische Verfahrensregelungen, die im Falle einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.

§ 30
Verarbeitung zu anderen Zwecken

(1) Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen in § 26 Abs. 1 genannten Zweck handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist.

(2) Absatz 1 gilt nicht für die Verarbeitung personenbezogener Daten, die einem Berufsgeheimnis oder einem besonderen Amtsgeheimnis unterliegen und der datenverarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden sind.

(3) Die Verarbeitung personenbezogener Daten zu einem anderen, in § 26 Abs. 1 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

(4) § 7 Abs. 5 gilt entsprechend.

§ 31
Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken

(1) Die Verarbeitung durch denselben oder einen anderen Verantwortlichen kann die Archivierung im öffentlichen Interesse und die wissenschaftliche, statistische oder historische Verwendung für die in § 26 Abs. 1 genannten

Zwecke umfassen, sofern geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen werden.

(2) Geeignete Garantien im Sinne des Absatzes 1 können in einer Anonymisierung der personenbezogenen Daten, in Vorkehrungen gegen ihre unbefugte Kenntnisnahme durch Dritte oder in ihrer räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeitung bestehen.

§ 32
Nachweis der Einhaltung durch den Verantwortlichen

Der Verantwortliche ist für die Einhaltung der in den §§ 28, 30 und 31 geregelten Bestimmungen verantwortlich und hat deren Einhaltung nachzuweisen.

§ 33
Einwilligung

(1) Soweit die Verarbeitung personenbezogener Daten nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von anderen Sachverhalten klar zu unterscheiden ist.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person ist vor Abgabe der Einwilligung durch den Verantwortlichen hiervon in Kenntnis zu setzen.

(4) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Ist dies nach den Umständen des Einzelfalls erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

(5) Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

§ 34
Verarbeitung auf Weisung des Verantwortlichen

Jede einem Verantwortlichen oder einem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten

ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach einer Rechtsvorschrift zur Verarbeitung verpflichtet ist.

§ 35
Datengeheimnis

(1) Den bei dem Verantwortlichen oder in dessen Auftrag beschäftigten Personen, die dienstlichen Zugang zu personenbezogenen Daten haben, ist es untersagt, diese Daten zu einem anderen als dem zur jeweiligen Aufgabenerfüllung gehörenden Zweck zu verarbeiten oder unbefugt zu offenbaren (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

(2) Die in Absatz 1 Satz 1 genannten Personen sind bei der Aufnahme ihrer Tätigkeit über ihre Pflichten nach Absatz 1 sowie die sonstigen bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten und auf deren Einhaltung zu verpflichten.

§ 36
Automatisierte Einzelentscheidung

(1) Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist, die geeignete Garantien für die Rechtsgüter der betroffenen Person bietet, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen.

(2) Entscheidungen nach Absatz 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechtsgüter sowie berechtigter Interessen der betroffenen Person getroffen wurden.

(3) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

Abschnitt 3
Datenschutzbeauftragte öffentlicher Stellen

§ 37
Benennung

(1) Öffentliche Stellen benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten.

(2) Für mehrere öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und Größe eine gemeinsame Datenschutzbeauftragte oder ein gemeinsamer Datenschutzbeauftragter benannt werden.

(3) Die oder der Datenschutzbeauftragte wird auf der Grundlage ihrer oder seiner beruflichen Qualifikation und insbesondere ihres oder seines Fachwissens benannt, das sie oder er auf dem Gebiet des Datenschutzrechts

und der Datenschutzpraxis besitzt, sowie auf der Grundlage ihrer oder seiner Fähigkeit zur Erfüllung der in § 39 genannten Aufgaben.

(4) Die oder der Datenschutzbeauftragte kann in einem Dienst- oder Beschäftigungsverhältnis mit der öffentlichen Stelle stehen oder ihre oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

(5) Die öffentliche Stelle veröffentlicht die Kontaktdaten der oder des Datenschutzbeauftragten und teilt diese Daten der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit mit.

§ 38
Stellung

(1) Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Die öffentliche Stelle unterstützt die Datenschutzbeauftragte oder den Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben gemäß § 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung ihres oder seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

(3) Die öffentliche Stelle stellt sicher, dass die oder der Datenschutzbeauftragte bei der Erfüllung ihrer oder seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Die oder der Datenschutzbeauftragte berichtet unmittelbar der höchsten Leitungsebene der öffentlichen Stelle. Die oder der Datenschutzbeauftragte darf von der öffentlichen Stelle wegen der Erfüllung ihrer oder seiner Aufgaben nicht abberufen oder benachteiligt werden.

(4) Die Abberufung der oder des Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

(5) Betroffene Personen können die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu allen Fragen in Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte nach Teil 3 dieses Gesetzes zu Rate ziehen. Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Personen sowie über Umstände, die Rückschlüsse auf die betroffenen Personen zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffenen Personen befreit wird.

(6) Wenn die oder der Datenschutzbeauftragte bei ihrer oder seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein

Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch der oder dem Datenschutzbeauftragten und den ihr oder ihm unterstellten, in einem Dienst- oder Beschäftigungsverhältnis mit der öffentlichen Stelle stehenden Personen zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

§ 39
Aufgaben

(1) Der oder dem Datenschutzbeauftragten obliegen im Anwendungsbereich des Teils 3 dieses Gesetzes folgende Aufgaben:

1. Unterrichtung und Beratung der öffentlichen Stelle und der mit ihr in einem Dienst- oder Beschäftigungsverhältnis stehenden Personen, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften,

2. Überwachung der Einhaltung dieses Gesetzes oder sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, sowie der Strategien der öffentlichen Stelle für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der an den Verarbeitungsvorgängen beteiligten, in einem Dienst- oder Beschäftigungsverhältnis mit ihr stehenden Personen und der diesbezüglichen Überprüfungen,

3. Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß § 56,

4. Zusammenarbeit mit der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit,

5. Tätigkeit als Anlaufstelle für die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß § 57, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Im Falle einer oder eines bei einem Gericht bestellten Datenschutzbeauftragten beziehen sich diese Aufgaben nicht auf das Handeln des Gerichts im Rahmen seiner justiziellen Tätigkeit.

(2) Die oder der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Die öffentliche Stelle stellt sicher, dass derartige Aufgaben nicht zu einem Interessenkonflikt führen.

(3) Die oder der Datenschutzbeauftragte trägt bei der Erfüllung ihrer oder seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei sie oder er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Abschnitt 4
Landesbeauftragte oder Landesbeauftragter für den Datenschutz und die Informationsfreiheit

§ 40
Rechtsstellung und Organisation

Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist Aufsichtsbehörde im Sinne des Artikels 41 der Richtlinie (EU) 2016/680 im Falle der Verarbeitung von Daten nach Teil 3 dieses Gesetzes. Die §§ 14, 15 und 18 finden hinsichtlich der Rechtsstellung und Organisation der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit entsprechende Anwendung.

§ 41
Aufgaben

(1) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat die folgenden Aufgaben:

1. die Anwendung dieses Gesetzes und die zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften zu überwachen und durchzusetzen,

2. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und aufzuklären,

3. den Landtag, die im Landtag vertretenen Fraktionen, die Landesregierung, die Kommunen und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten,

4. die Verantwortlichen und die Auftragsverarbeiter für die ihnen nach diesem Gesetz sowie aus den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften bestehenden Pflichten zu sensibilisieren,

5. auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer nach Maßgabe dieses Gesetzes und der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften zur Verfügung

zu stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenzuarbeiten,

6. sich mit Beschwerden einer betroffenen Person oder einer Stelle, einer Organisation oder eines Verbands gemäß § 50 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist,

7. mit anderen Aufsichtsbehörden zusammenzuarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung der Richtlinie (EU) 2016/680 zu gewährleisten,

8. Untersuchungen über die Anwendung dieses Gesetzes und der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde,

9. maßgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie,

10. Beratung in Bezug auf die in § 57 genannten Verarbeitungsvorgänge zu leisten,

11. die Aufgaben nach § 45 Abs. 7 und § 48 wahrzunehmen.

(2) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist nicht zuständig für die Aufsicht über die von den Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

(3) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit erleichtert das Einreichen der in Absatz 1 Nr. 6 genannten Beschwerden durch Maßnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

(4) Die Erfüllung der Aufgaben erfolgt für die betroffene Person und für die Datenschutzbeauftragte oder den Datenschutzbeauftragten unentgeltlich. Bei offenkundig unbegründeten oder besonders wegen häufiger Wiederholung exzessiven Anträgen kann die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit eine angemessene Gebühr verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall trägt die oder der Landesbeauftragte für den Datenschutz und die

Informationsfreiheit die Beweislast dafür, dass der Antrag offenkundig unbegründet oder exzessiv ist.

(5) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit erstellt einen Jahresbericht über ihre oder seine Tätigkeit, der eine Liste der Arten der gemeldeten Verstöße und der Arten der verhängten Sanktionen enthalten kann. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit übermittelt den Bericht dem Landtag sowie der Landesregierung und macht ihn der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich. § 16 Abs. 3 findet entsprechende Anwendung.

§ 42
Befugnisse

(1) Stellt die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit bei Datenverarbeitungen Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten zu Zwecken des § 26 Abs. 1 fest, so beanstandet sie oder er dies im Falle einer öffentlichen Stelle

1. des Landes gegenüber der zuständigen obersten Landesbehörde,

2. einer Gemeinde, eines Gemeindeverbands, eines Landkreises oder einer sonstigen der Aufsicht des Landes oder einer Gemeinde, eines Gemeindeverbands oder eines Landkreises unterstehenden Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts sowie einer Vereinigung einer solchen Körperschaft, Anstalt oder Stiftung gegenüber dem vertretungsberechtigten Organ

und fordert eine Stellungnahme innerhalb einer angemessenen Frist ein. In den Fällen des Satzes 1 Nr. 2 unterrichtet die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit gleichzeitig die zuständige Aufsichtsbehörde. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit getroffen worden sind. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit kann den Verantwortlichen auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstoßen.

(2) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit kann bei Verstößen nach Absatz 1 Satz 1 darüber hinaus anordnen,

1. Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise oder innerhalb eines bestimmten Zeitraums, mit den Bestimmungen dieses Gesetzes oder anderen Vorschriften über den Datenschutz in Einklang zu bringen,

2. personenbezogene Daten zu berichtigen,

3. personenbezogene Daten in der Verarbeitung einzuschränken,

4. personenbezogene Daten zu löschen,

wenn dies zur Beseitigung eines erheblichen Verstoßes gegen datenschutzrechtliche Vorschriften erforderlich ist.

(3) Die öffentlichen Stellen sind verpflichtet, die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Ihr oder ihm sind insbesondere

1. Auskunft zu allen Fragen zu erteilen und alle Dokumente vorzulegen, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen,

2. Zugang zu allen personenbezogenen Daten, die verarbeitet werden, zu gewähren, und

3. Zugang zu den Grundstücken und Diensträumen einschließlich aller Datenverarbeitungsanlagen und -geräte zu gewähren, soweit dies zur Erfüllung ihrer oder seiner Aufgaben erforderlich ist.

(4) Die Verpflichtung nach Absatz 3 entfällt, soweit eine oberste Landesbehörde im Einzelfall feststellt, dass die Sicherheit des Bundes oder eines Landes dies gebietet. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit ist hierüber schriftlich zu informieren. Die Gründe hierfür sind aktenkundig zu machen.

Abschnitt 5
Rechte der betroffenen Person

§ 43
Allgemeine Informationen zu Datenverarbeitungen

Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich folgende Informationen zur Verfügung zu stellen:

1. die Zwecke der von ihm vorgenommenen Verarbeitungen,

2.

die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,

3. den Namen und die Kontaktdaten des Verantwortlichen und der oder des Datenschutzbeauftragten,

4. Hinweis auf die Befugnis, die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit anzurufen und

5. Angaben zur Erreichbarkeit der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit.

§ 44
Benachrichtigung betroffener Personen

(1) Ist die Benachrichtigung betroffener Personen über die Verarbeitung sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Maßnahmen, vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten:

1. die in § 43 genannten Angaben,

2. die Rechtsgrundlage der Verarbeitung,

3. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Fristen,

4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie

5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) In den Fällen des Absatzes 1 kann der Verantwortliche die Benachrichtigung insoweit und solange aufschieben, einschränken und unterlassen, wie andernfalls

1. die Erfüllung der in § 26 Abs. 1 genannten Aufgaben,

2. die öffentliche Sicherheit oder

3. Rechtsgüter Dritter

gefährdet würden, wenn das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt.

(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden des Bundes und der Länder, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Im Falle der Einschränkung nach Absatz 2 gilt § 45 Abs. 7 entsprechend.

§ 45
Auskunftsrecht

(1) Der Verantwortliche hat betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob er sie betreffende Daten verarbeitet. Betroffene Personen haben darüber hinaus das Recht, Informationen zu erhalten über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören,

2. die verfügbaren Informationen über die Herkunft der Daten,

3. die Zwecke der Verarbeitung und deren Rechtsgrundlage,

4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen,

5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen,

7. das Recht, nach § 48 die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit anzurufen sowie

8. Angaben zur Erreichbarkeit der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder die ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist.

(3) Von der Auskunftserteilung ist abzusehen, soweit die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Der betroffenen Person ist vor dem Absehen der Auskunftserteilung Gelegenheit zur Präzisierung des Auskunftsersuchens zu geben.

(4) Der Verantwortliche kann unter den Voraussetzungen des § 44 Abs. 2 von der Auskunft nach Absatz 1 Satz 1 absehen oder die Auskunftserteilung nach Absatz 1 Satz 2 teilweise oder vollständig einschränken.

(5) § 44 Abs. 3 gilt entsprechend.

(6) Der Verantwortliche hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 44 Abs. 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährden würde.

(7) Wird die betroffene Person nach Absatz 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie gemäß § 48 die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit anrufen oder gerichtlichen Rechtsschutz suchen kann. Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, soweit nicht die zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Wird der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit eine Auskunft nicht erteilt, so sind die Gründe dafür aktenkundig zu machen. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat die betroffene Person zumindest darüber zu unterrichten, dass eine Überprüfung durch sie oder ihn stattgefunden hat. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. Die Mitteilung der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Der Verantwortliche darf die Zustimmung nur insoweit und solange verweigern, wie er nach Absatz 4 von einer Auskunft absehen oder sie einschränken könnte. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

(8) Der Verantwortliche hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

§ 46
Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Beurteilung, sondern die Tatsache, dass die Aussage oder Beurteilung so erfolgt ist. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem unter Berücksichtigung der Verarbeitungszwecke die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies angemessen ist.

(2) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn deren Verarbeitung unzulässig ist, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

(3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde,

2. die Daten zu Beweiszwecken in Verfahren, die den in § 26 Abs. 1 genannten Zwecken dienen, weiter aufbewahrt werden müssen oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand.

(4) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

(5) Hat der Verantwortliche eine Berichtigung vorgenommen, hat er einer Stelle, die ihm die personenbezogenen Daten übermittelt hat, die Berichtigung mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken. In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1 bis 3 hat der Verantwortliche anderen Empfängern, denen die Daten übermittelt wurden, diese Maßnahmen mitzuteilen.

(6) Der Verantwortliche hat die betroffene Person über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 44 Abs. 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde.

(7) § 45 Abs. 7 und 8 findet entsprechende Anwendung.

§ 47
Verfahren für die Ausübung der Rechte der betroffenen Person

(1) Der Verantwortliche hat mit betroffenen Personen unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren.

(2) Bei Anträgen hat der Verantwortliche die betroffene Person unbeschadet des § 45 Abs. 6 und des § 46 Abs. 6 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde.

(3) Die Erteilung von Informationen nach § 43, Benachrichtigungen nach den §§ 44 und 55 sowie die Bearbeitung von Anträgen nach den §§ 45 und 46 erfolgen unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 45 und 46 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage von Verwaltungskosten verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.

(4) Hat der Verantwortliche begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach § 45 oder § 46 gestellt hat, kann er von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 48
Anrufung der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Jede betroffene Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen zu den in § 26 Abs. 1 genannten Zwecken in ihren Rechten verletzt worden zu sein. Dies gilt nicht für die Verarbeitung von personenbezogenen Daten durch Gerichte, soweit diese die Daten im Rahmen ihrer justiziellen Tätigkeit verarbeitet haben. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat die betroffene Person über den Stand und das Ergebnis der Beschwerde

zu unterrichten und sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes nach § 49 hinzuweisen.

(2) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer Aufsichtsbehörde in einem anderen Mitgliedstaat der Europäischen Union fällt, unverzüglich an die zuständige Aufsichtsbehörde des anderen Staates weiterzuleiten. Sie oder er hat in diesem Fall die betroffene Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

§ 49
Rechtsschutz gegen Entscheidungen der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit oder bei deren oder dessen Untätigkeit

(1) Jede natürliche oder juristische Person kann unbeschadet anderer Rechtsbehelfe gerichtlich gegen eine verbindliche Entscheidung der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit vorgehen.

(2) Absatz 1 gilt entsprechend zugunsten betroffener Personen, wenn sich die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit mit einer Beschwerde nach § 48 nicht befasst oder die betroffene Person nicht innerhalb von drei Monaten nach Einlegung der Beschwerde über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.

§ 50
Vertretung von betroffenen Personen

Die betroffene Person kann eine rechtmäßig gegründete Einrichtung, Organisation oder Vereinigung ohne Gewinnerzielungsabsicht, deren satzungsmäßige Ziele im öffentlichen Interesse liegen und die im Bereich des Schutzes der Rechtsgüter betroffener Personen in Bezug auf den Schutz personenbezogener Daten tätig ist, beauftragen, im Namen der betroffenen Person eine Beschwerde einzureichen oder die Rechte nach § 45 Abs. 1 Satz 2 Nr. 7 sowie nach den §§ 48 und 49 wahrzunehmen.

Abschnitt 6
Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 51
Auftragsverarbeitung

(1) Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Bestimmungen dieses Gesetzes und anderer Vorschriften über den Datenschutz zu sorgen. Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und

Schadensersatz sind in diesem Fall gegenüber dem Verantwortlichen geltend zu machen.

(2) Ein Verantwortlicher darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

(3) Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung des Verantwortlichen keinen weiteren Auftragsverarbeiter hinzuziehen. Hat der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzuziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. Der Verantwortliche kann in diesem Fall die Hinzuziehung oder Ersetzung untersagen.

(4) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit dem Verantwortlichen nach Absatz 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Vorschriften verbindlich sind. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

(5) Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter

1. nur auf dokumentierte Weisung des Verantwortlichen handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er den Verantwortlichen unverzüglich zu informieren;

2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

3. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;

4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt

oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;

5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die gemäß § 64 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;

6. Überprüfungen, die von dem Verantwortlichen oder einem anderen, von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt;

7. die in den Absätzen 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

8. alle gemäß § 53 erforderlichen Maßnahmen ergreift und

9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den §§ 53 bis 57 genannten Pflichten unterstützt.

(6) Der Vertrag im Sinne des Absatzes 5 ist schriftlich oder elektronisch abzufassen.

(7) Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoß gegen diese Bestimmung festlegt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

§ 52
Gemeinsam Verantwortliche

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als gemeinsam Verantwortliche. Gemeinsam Verantwortliche haben ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung festzulegen, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind. Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen Informationspflichten nachzukommen hat und wie und gegenüber wem betroffene Personen ihre Rechte wahrnehmen können. Eine entsprechende Vereinbarung hindert die betroffene Person nicht, ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen.

§ 53
Anforderungen an die Sicherheit der Datenverarbeitung

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der

Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und

2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

(3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen zu ergreifen, die Folgendes bezwecken:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),

2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),

5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle),

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten mit Hilfe von Einrichtungen

zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),

7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),

8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit),

10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),

11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),

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

13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Ein Zweck nach Satz 1 Nr. 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

§ 54
Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihm bekannt geworden ist, der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit zu melden, es sei denn, dass die Verletzung voraussichtlich kein Risiko für die Rechtsgüter natürlicher Personen mit sich gebracht hat. Erfolgt die Meldung an die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die

Informationsfreiheit nicht innerhalb von 72 Stunden, so ist die Verzögerung zu begründen.

(2) Ein Auftragsverarbeiter hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen zu melden.

(3) Die Meldung nach Absatz 1 hat zumindest folgende Informationen zu enthalten:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,

2. den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann,

3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung und der getroffenen Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn die Informationen nach Absatz 3 nicht zusammen mit der Meldung übermittelt werden können, hat der Verantwortliche sie unverzüglich nachzureichen, sobald sie ihm vorliegen.

(5) Der Verantwortliche hat die Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen zu umfassen.

(6) Soweit von einer Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von einem oder an einen Verantwortlichen in einem anderen Mitgliedstaat der Europäischen Union übermittelt wurden, sind die in Absatz 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

(7) § 42 Abs. 4 BDSG findet entsprechende Anwendung.

(8) Weitere Pflichten des Verantwortlichen zu Benachrichtigungen über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

§ 55
Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

(1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich über den Vorfall zu benachrichtigen.

(2) Die Benachrichtigung nach Absatz 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in § 54 Abs. 3 Nr. 2 bis 4 genannten Informationen und Maßnahmen zu enthalten.

(3) Von einer Benachrichtigung nach Absatz 1 kann abgesehen werden, wenn

1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht wurden,

2. der Verantwortliche durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach kein hohes Risiko im Sinne des Absatzes 1 mehr besteht, oder

3. dies mit einem unverhältnismäßigen Aufwand verbunden wäre; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

(4) Wenn der Verantwortliche die betroffenen Personen über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt hat, kann die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit förmlich feststellen, dass ihrer oder seiner Auffassung nach die in Absatz 3 genannten Voraussetzungen nicht erfüllt sind. Hierbei hat sie oder er die Wahrscheinlichkeit zu berücksichtigen, dass die Verletzung ein hohes Risiko zur Folge hat.

(5) Die Benachrichtigung der betroffenen Person nach Absatz 1 kann unter den in § 44 Abs. 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund der von der Verletzung ausgehenden hohen Risiken überwiegen. Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden des Bundes und der Länder, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst, ist sie nur mit Zustimmung dieser Stellen zulässig.

(6) § 42 Abs. 4 BDSG findet entsprechende Anwendung.

§ 56
Durchführung einer
Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen (Datenschutz-Folgenabschätzung).

(2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

(3) Der Verantwortliche hat die Datenschutzbeauftragte oder den Datenschutzbeauftragten an der Durchführung der Datenschutz-Folgenabschätzung zu beteiligen.

(4) Die Datenschutz-Folgenabschätzung hat den Rechten der von der Datenverarbeitung betroffenen Personen und sonstiger Betroffener Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und den Zweck der Verarbeitung,

2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck,

3. eine Bewertung der Risiken für die Rechtsgüter der betroffenen Personen und

4. die Maßnahmen, mit denen bestehenden Risiken abgeholfen werden soll, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.

(5) Soweit erforderlich hat der Verantwortliche eine Überprüfung durchzuführen, ob die Verarbeitung den Maßgaben folgt, die sich aus der Datenschutz-Folgenabschätzung ergeben haben.

§ 57
Konsultation der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit zu konsultieren, wenn

1. aus der Datenschutz-Folgenabschätzung nach § 56 hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechtsgüter der betroffenen Personen zur Folge hätte, wenn der Verantwortliche keine Abhilfemaßnahmen treffen würde oder

2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren ein hohes Risiko für die Rechtsgüter der betroffenen Personen zur Folge hat.

Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen.

(2) Bei der Ausarbeitung eines Vorschlags für die Datenverarbeitung betreffende Gesetzes- und Verordnungsentwürfe ist zuvor die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit zu konsultieren.

(3) Der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit sind im Falle des Absatzes 1 vorzulegen:

1. die nach § 56 durchgeführte Datenschutz-Folgenabschätzung,

2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter,

3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung,

4. Angaben zu den zum Schutz der Rechtsgüter der betroffenen Person vorgesehenen Maßnahmen und Garantien,

5. Name und Kontaktdaten der oder des Datenschutzbeauftragten.

Auf Anforderung sind ihr oder ihm zudem alle sonstigen Informationen zu übermitteln, die sie oder er benötigt, um die Rechtmäßigkeit der Verarbeitung sowie insbesondere die in Bezug auf den Schutz der personenbezogenen Daten der betroffenen Person bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

(4) Falls die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. Sie oder er hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zu informieren.

(5) Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Absatz 4 Satz 1 genannten Frist beginnen. In diesem Fall sind die Empfehlungen der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

§ 58
Verzeichnis von Verarbeitungstätigkeiten

(1) Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen. Dieses Verzeichnis hat folgende Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls die gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten,

2. die Zwecke der Verarbeitung,

3. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden,

4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,

5. gegebenenfalls die Verwendung von Profiling,

6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,

7. Angaben über die Rechtsgrundlage der Verarbeitung einschließlich der Übermittlungen, für die die personenbezogenen Daten bestimmt sind,

8. wenn möglich die vorgesehenen Fristen für die Löschung der verschiedenen Kategorien personenbezogener Daten,

9. wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 53.

(2) Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen zu führen, die er im Auftrag eines Verantwortlichen durchführt, das Folgendes zu enthalten hat:

1.

den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist sowie gegebenenfalls der oder des Datenschutzbeauftragten,

2. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,

3. gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,

4. wenn möglich eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß § 53.

(3) Die in den Absätzen 1 und 2 genannten Verzeichnisse sind schriftlich oder elektronisch zu führen.

(4) Verantwortliche und Auftragsverarbeiter haben auf Anforderung ihre Verzeichnisse der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit zur Verfügung zu stellen.

§ 59
Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. Er hat hierbei den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen. Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist.

(2) Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Maßnahmen müssen insbesondere gewährleisten, dass die Daten durch Voreinstellungen nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

§ 60
Unterscheidung zwischen verschiedenen Kategorien betroffener Personen

Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Dies betrifft insbesondere folgende Kategorien:

1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben,

2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden,

3. verurteilte Straftäterinnen und Straftäter,

4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und

5. andere Personen wie insbesondere Zeugen, Hinweisgeber oder Personen, die mit den in den Nummern 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

§ 61
Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen

Der Verantwortliche hat bei der Verarbeitung so weit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. Es muss außerdem feststellbar sein, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen.

§ 62
Verfahren bei Übermittlungen

(1) Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht mehr übermittelt oder sonst zur Verfügung gestellt werden. Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. Bei jeder Übermittlung personenbezogener Daten hat er zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

(2) Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger auf diese Bedingungen hinzuweisen. Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend markiert werden.

(3) Die übermittelnde Stelle darf auf Empfänger in anderen Mitgliedstaaten der Europäischen Union auf Einrichtungen und sonstige Stellen, die nach den Kapiteln 4 und 5 des Titels V des Dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union errichtet wurden, keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

(4) § 5 Abs. 2 gilt entsprechend.

§ 63
Berichtigung und Löschung sowie Einschränkung der Verarbeitung

(1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Eine Berichtigung ist der Stelle, die die Daten zuvor übermittelt hat, mitzuteilen.

(2) Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist.

(3) § 46 Abs. 1 Satz 3 und Abs. 3 bis 5 ist entsprechend anzuwenden. Sind personenbezogene Daten unrechtmäßig übermittelt worden, ist dies auch dem Empfänger mitzuteilen.

(4) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder eine regelmäßige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

§ 64
Protokollierung

(1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren:

1. Erhebung,

2. Veränderung,

3. Abfrage,

4. Offenlegung einschließlich Übermittlung,

5. Kombination und

6. Löschung.

(2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum, die Uhrzeit dieser Vorgänge, so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen. Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit auf Anforderung zur Verfügung zu stellen.

(3) Die Protokolle dürfen ausschließlich für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung, die Eigenüberwachung, die Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten sowie für Strafverfahren verwendet werden.

(4) Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen.

(5) Für vor dem 6. Mai 2016 eingerichtete automatisierte Verarbeitungssysteme kann die Umsetzung der Vorgaben der Absätze 1 bis 4 in Ausnahmefällen bis längstens zum 6. Mai 2023 aufgeschoben werden, wenn die technische Umsetzung mit einem unverhältnismäßigen Aufwand verbunden ist.

§ 65
Vertrauliche Meldung von Verstößen

Der Verantwortliche hat wirksame Vorkehrungen zu treffen, um vertrauliche Meldungen über Verstöße gegen das geltende Recht zu fördern.

Abschnitt 7
Datenübermittlung an Drittstaaten und an internationale Organisationen

§ 66
Allgemeine Voraussetzungen

(1) Die Übermittlung personenbezogener Daten an Stellen in Drittstaaten oder an internationale Organisationen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn

1. die Übermittlung für die in § 26 Abs. 1 genannten Zwecke erforderlich ist,

2. die Stelle oder Organisation für die in § 26 Abs. 1 genannten Zwecke zuständig ist und

3. die Europäische Kommission gemäß Artikel 36 Abs. 1 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat oder, wenn kein solcher Beschluss vorliegt, geeignete Garantien im Sinne des § 67 erbracht wurden oder bestehen, oder, wenn weder ein solcher Beschluss noch geeignete Garantien vorliegen, Ausnahmen für bestimmte Fälle gemäß § 68 anwendbar sind.

(2) Die Übermittlung personenbezogener Daten hat trotz des Vorliegens eines Angemessenheitsbeschlusses im Sinne des Absatzes 1 Nr. 3 und des zu berücksichtigenden öffentlichen Interesses an der Datenübermittlung zu unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Menschenrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen. Bei seiner Beurteilung hat der Verantwortliche maßgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

(3) Wenn personenbezogene Daten, die aus einem anderen Mitgliedstaat der Europäischen Union übermittelt oder zur Verfügung gestellt wurden, nach Absatz 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der zuständigen Stelle des anderen Mitgliedstaats genehmigt werden. Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Im Falle des Satzes 2 ist die Stelle des anderen Mitgliedstaats, die für die Erteilung der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

(4) Der Verantwortliche, der Daten nach Absatz 1 übermittelt, hat durch geeignete Maßnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere internationale Organisationen weiterübermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat. Bei der Entscheidung über die Erteilung der Genehmigung hat der Verantwortliche alle maßgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittstaat oder der internationalen Organisation, an den oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbezogene Daten. Eine Genehmigung darf nur dann erfolgen, wenn auch eine direkte Übermittlung an den anderen Drittstaat oder die andere internationale Organisation zulässig wäre. Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

§ 67
Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 66 Abs. 1 Nr. 3 kein Beschluss nach Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 66 auch dann zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder

2. der Verantwortliche nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, zu der Auffassung gelangt ist, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

(2) Der Verantwortliche hat Übermittlungen nach Absatz 1 Nr. 2 zu dokumentieren. Die Dokumentation hat den Zeitpunkt der Übermittlung, die Identität des Empfängers, den Grund der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. Sie ist der oder dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit auf Anforderung zur Verfügung zu stellen.

(3) Der Verantwortliche hat die Landesbeauftragte oder den Landesbeauftragten für den Datenschutz und die Informationsfreiheit zumindest jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Absatz 1 Nr. 2 erfolgt sind. In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

§ 68
Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 66 Abs. 1 Nr. 3 kein Beschluss nach Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 67 Abs. 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 66 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,

2. zur Wahrung berechtigter Interessen der betroffenen Person, wenn dies nach dem geltenden Recht des Mitgliedstaats, aus dem die personenbezogenen Daten übermittelt werden, vorgesehen ist,

3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit des Staates,

4. im Einzelfall für die in § 26 Abs. 1 genannten Zwecke oder

5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 26 Abs. 1 genannten Zwecken.

(2) Der Verantwortliche hat von einer Übermittlung nach Absatz 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung im Sinne des Absatzes 1 Nr. 4 und 5 überwiegen.

(3) Für Übermittlungen nach Absatz 1 gilt § 67 Abs. 2 und 3 entsprechend.

§ 69
Sonstige Datenübermittlungen an Empfänger in Drittstaaten

(1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 66 Abs. 1 Nr. 2 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen,

2. die Übermittlung an die in § 66 Abs. 1 Nr. 2 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und

3. der Verantwortliche dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

(2) Im Fall des Absatzes 1 hat der Verantwortliche die in § 66 Abs. 1 Nr. 2 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Absatz 1 gilt § 67 Abs. 2 und 3 entsprechend.

(4) Bei Übermittlungen nach Absatz 1 hat der Verantwortliche den Empfänger zu verpflichten, die übermittelten personenbezogenen Daten ohne seine Zustimmung nur für den Zweck zu verarbeiten, für den sie übermittelt worden sind.

(5) Abkommen im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit bleiben unberührt.

Abschnitt 8
Zusammenarbeit der Aufsichtsbehörden

§ 70
Gegenseitige Amtshilfe

(1) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat den Datenschutzaufsichtsbehörden in anderen Mitgliedstaaten der Europäischen Union Informationen zu übermitteln und Amtshilfe zu leisten, soweit dies für eine einheitliche Umsetzung und Anwendung der Richtlinie (EU) 2016/680 erforderlich ist. Die Amtshilfe betrifft insbesondere Auskunftsersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat alle geeigneten Maßnahmen zu ergreifen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingang nachzukommen. Dazu kann insbesondere auch die Übermittlung maßgeblicher Informationen über die Durchführung einer Untersuchung gehören.

(3) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit darf Amtshilfeersuchen nur ablehnen, wenn

1. sie oder er für den Gegenstand des Ersuchens oder für die Maßnahmen, die sie oder er durchführen soll, nicht zuständig ist oder

2. ein Eingehen auf das Ersuchen gegen Rechtsvorschriften verstoßen würde.

(4) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat die ersuchende Aufsichtsbehörde des anderen Staates über die Ergebnisse oder gegebenenfalls über den Fortgang der Maßnahmen zu informieren, die getroffen wurden, um dem Amtshilfeersuchen nachzukommen. Sie oder er hat im Falle des Absatzes 3 die Gründe für die Ablehnung des Ersuchens zu erläutern.

(5) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat die Informationen, um die von einer anderen Aufsichtsbehörde ersucht wurde, in der Regel auf elektronischem Weg unter Verwendung eines standardisierten Formulars zu übermitteln.

(6) Die oder der Landesbeauftragte für den Datenschutz und die Informationsfreiheit hat Amtshilfeersuchen kostenfrei zu erledigen, soweit sie oder er nicht im Einzelfall mit der Aufsichtsbehörde des anderen Staates die Erstattung entstandener Ausgaben vereinbart hat.

(7) Ein Amtshilfeersuchen der oder des Landesbeauftragten für den Datenschutz und die Informationsfreiheit hat alle erforderlichen Informationen zu enthalten; hierzu gehören insbesondere der Zweck und die Begründung des Ersuchens. Die auf das Ersuchen übermittelten Informationen dürfen ausschließlich zu dem Zweck verwendet werden, zu dem sie angefordert wurden.

Abschnitt 9
Haftung und Sanktionen

§ 71
Schadensersatz

(1) Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder anderen auf ihre Verarbeitung anwendbaren Vorschriften rechtswidrig war, einen Schaden zugefügt, ist er oder sein Rechtsträger der betroffenen Person zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einer

nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.

(2) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

(3) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welcher von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche beziehungsweise sein Rechtsträger.

(4) Mehrere Ersatzpflichtige haften gesamtschuldnerisch.

(5) Hat bei der Entstehung des Schadens ein Verschulden der betroffenen Person mitgewirkt, ist § 254 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

(6) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

(7) Die Geltendmachung weitergehender Schadensersatzansprüche aufgrund anderer Rechtsvorschriften bleibt unberührt.

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

§ 72
Ordnungswidrigkeiten und Strafbestimmungen

Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten nach § 26 Abs. 1 Satz 1 finden die §§ 24 und 25 entsprechende Anwendung.

Teil 4
Übergangs- und Schlussbestimmungen

§ 73
Verweisungen und Bezeichnungen in anderen Vorschriften

Soweit in anderen Vorschriften auf Bestimmungen verwiesen wird, die durch dieses Gesetz außer Kraft gesetzt werden, oder Bezeichnungen verwendet werden, die durch dieses Gesetz aufgehoben oder geändert werden, treten an deren Stelle die entsprechenden Bestimmungen und Bezeichnungen dieses Gesetzes.

§ 74
Inkrafttreten

(1) Dieses Gesetz tritt am 25. Mai 2018 in Kraft.

(2) Gleichzeitig tritt das Landesdatenschutzgesetz vom 5. Juli 1994 (GVBl. S. 293), zuletzt geändert durch Artikel 2 des Gesetzes vom 20. Dezember 2011 (GVBl. S. 427), BS 204-1, außer Kraft.

Mainz, den 8. Mai 2018
Die Ministerpräsidentin
Malu Dreyer