


Amtliche Abkürzung: HDSIG
Ausfertigungsdatum: 03.05.2018
Gültig ab: 25.05.2018
Dokumenttyp: Gesetz
Quelle: 
Fundstelle: GVBl. 2018, 82
Gliederungs-Nr: 300-47

Hessisches Datenschutz- und Informationsfreiheitsgesetz
(HDSIG)
Vom 3. Mai 2018^{*)}

Zum 20.10.2022 aktuellste verfügbare Fassung der Gesamtausgabe

Stand: letzte berücksichtigte Änderung: Inhaltsübersicht sowie §§ 81 und 88 geändert, § 28c neu eingefügt durch Artikel 9 des Gesetzes vom 15. November 2021 (GVBl. S. 718, 729)

Fußnoten

- *) Verkündet als Artikel 1 des Hessischen Gesetzes zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU) Nr. 2016/680 und zur Informationsfreiheit vom 3. Mai 2018 (GVBl. S. 82)

Nichtamtliches Inhaltsverzeichnis

Titel	Gültig ab
Hessisches Datenschutz- und Informationsfreiheitsgesetz (HDSIG) vom 3. Mai 2018	25.05.2018
Inhaltsverzeichnis	01.01.2022
ERSTER TEIL - Gemeinsame Bestimmungen	25.05.2018
Erster Abschnitt - Anwendungsbereich und Begriffsbestimmungen	25.05.2018
§ 1 - Anwendungsbereich	25.05.2018
§ 2 - Begriffsbestimmungen	25.05.2018
Zweiter Abschnitt - Rechtsgrundlagen für die Verarbeitung personenbezogener Daten	25.05.2018
§ 3 - Verarbeitung personenbezogener Daten, Auftragsverarbeitung	25.05.2018
§ 4 - Videoüberwachung öffentlich zugänglicher Räume	25.05.2018
Dritter Abschnitt - Datenschutzbeauftragte öffentlicher Stellen	25.05.2018
§ 5 - Benennung	25.05.2018
§ 6 - Rechtsstellung	25.05.2018
§ 7 - Aufgaben	25.05.2018

Titel	Gültig ab
Vierter Abschnitt - Die oder der Hessische Datenschutzbeauftragte	25.05.2018
§ 8 - Rechtsstellung und Unabhängigkeit	25.05.2018
§ 9 - Wahl	25.05.2018
§ 10 - Persönliche Voraussetzungen	25.05.2018
§ 11 - Amtsverhältnis	25.05.2018
§ 12 - Verschwiegenheitspflicht	25.05.2018
§ 13 - Zuständigkeit und Aufgaben	25.05.2018
§ 14 - Befugnisse	25.05.2018
§ 15 - Gutachten und Untersuchungen, Tätigkeitsbericht	25.05.2018
§ 16 - Informationspflichten	25.05.2018
§ 17 - Benachteiligungsverbot bei Anrufung der oder des Hessischen Datenschutzbeauftragten	25.05.2018
§ 18 - Personal- und Sachausstattung	25.05.2018
Fünfter Abschnitt - Rechtsbehelfe	25.05.2018
§ 19 - Gerichtlicher Rechtsschutz	25.05.2018
ZWEITER TEIL - Durchführungsbestimmungen für Verarbeitungen zu Zwecken nach Artikel 2 der Verordnung (EU) Nr. 2016/679	25.05.2018
Erster Abschnitt - Rechtsgrundlagen der Verarbeitung personenbezogener Daten	25.05.2018
Erster Titel - Verarbeitung personenbezogener Daten und Verarbeitung zu anderen Zwecken	25.05.2018
§ 20 - Verarbeitung besonderer Kategorien personenbezogener Daten	25.05.2018
§ 21 - Verarbeitung zu anderen Zwecken	25.05.2018
§ 22 - Datenübermittlungen durch öffentliche Stellen	25.05.2018
Zweiter Titel - Besondere Verarbeitungssituationen	25.05.2018
§ 23 - Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses	25.05.2018
§ 24 - Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken	25.05.2018
§ 25 - Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken	25.05.2018
§ 26 - Rechte der betroffenen Person und auf sichtsbehördliche Untersuchungen im Fall von Geheimhaltungspflichten	25.05.2018
§ 27 - Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften	25.05.2018

Titel	Gültig ab
§ 28 - Datenverarbeitung des Hessischen Rundfunks zu journalistischen Zwecken	25.05.2018
§ 28a - Datenverarbeitung bei öffentlichen Auszeichnungen und Ehrungen	25.09.2018
§ 28b - Datenverarbeitung in Gnadenverfahren	25.09.2018
§ 28c - Datenübermittlung durch berufsständische Versorgungseinrichtungen	01.01.2022
Dritter Titel - Rechte des Landtags und der kommunalen Vertretungsorgane	25.05.2018
§ 29 - Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane	25.05.2018
§ 30 - Verarbeitung personenbezogener Daten durch den Landtag und die kommunalen Vertretungsorgane	25.05.2018
Zweiter Abschnitt - Rechte der betroffenen Person	25.05.2018
§ 31 - Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person	25.05.2018
§ 32 - Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden	25.05.2018
§ 33 - Auskunftsrecht der betroffenen Person	25.05.2018
§ 34 - Recht auf Löschung („Recht auf Vergessenwerden“)	25.05.2018
§ 35 - Widerspruchsrecht	25.05.2018
Dritter Abschnitt - Sanktionen	25.05.2018
§ 36 - Anwendung der Vorschriften über das Bußgeld- und Strafverfahren bei Verstößen nach Artikel 83 der Verordnung (EU) Nr. 2016/679	25.05.2018
§ 37 - Strafvorschriften	25.05.2018
§ 38 - Bußgeldvorschriften	25.05.2018
Vierter Abschnitt - Gemeinsame Verfahren, Gemeinsam Verantwortliche	25.05.2018
§ 39 - Gemeinsame Verfahren, Gemeinsam Verantwortliche	25.05.2018
DRITTER TEIL - Bestimmungen für Verarbeitungen zu Zwecken nach Artikel 1 Absatz 1 der Richtlinie (EU) Nr. 2016/680	25.05.2018
Erster Abschnitt - Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten	25.05.2018
§ 40 - Anwendungsbereich	25.05.2018
§ 41 - Begriffsbestimmungen	25.05.2018
§ 42 - Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten	25.05.2018
Zweiter Abschnitt - Rechtsgrundlagen für die Verarbeitung personenbezogener Daten	25.05.2018
§ 43 - Verarbeitung besonderer Kategorien personenbezogener Daten	25.05.2018

Titel	Gültig ab
§ 44 - Verarbeitung zu anderen Zwecken	25.05.2018
§ 45 - Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken, archivarischen oder statistischen Zwecken	25.05.2018
§ 46 - Einwilligung	25.05.2018
§ 47 - Verarbeitung auf Weisung des Verantwortlichen	25.05.2018
§ 48 - Datengeheimnis	25.05.2018
§ 49 - Automatisierte Einzelentscheidung	25.05.2018
Dritter Abschnitt - Rechte der betroffenen Person	25.05.2018
§ 50 - Allgemeine Informationen zu Datenverarbeitungen	25.05.2018
§ 51 - Benachrichtigung betroffener Personen	25.05.2018
§ 52 - Auskunftsrecht	25.05.2018
§ 53 - Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung	25.05.2018
§ 54 - Verfahren für die Ausübung der Rechte der betroffenen Person	25.05.2018
§ 55 - Anrufung der oder des Hessischen Datenschutzbeauftragten	25.05.2018
§ 56 - Rechtsschutz gegen Entscheidungen der oder des Hessischen Datenschutzbeauftragten oder bei deren oder dessen Untätigkeit	25.05.2018
Vierter Abschnitt - Pflichten der Verantwortlichen und Auftragsverarbeiter	25.05.2018
§ 57 - Auftragsverarbeitung	25.05.2018
§ 58 - Gemeinsame Verfahren, Gemeinsam Verantwortliche	25.05.2018
§ 59 - Anforderungen an die Sicherheit der Datenverarbeitung	25.05.2018
§ 60 - Meldung von Verletzungen des Schutzes personenbezogener Daten an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten	25.05.2018
§ 61 - Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten	25.05.2018
§ 62 - Durchführung einer Datenschutz-Folgenabschätzung	25.05.2018
§ 63 - Zusammenarbeit mit der oder dem Hessischen Datenschutzbeauftragten	25.05.2018
§ 64 - Vorherige Konsultation der oder des Hessischen Datenschutzbeauftragten	25.05.2018
§ 65 - Verzeichnis von Verarbeitungstätigkeiten	25.05.2018
§ 66 - Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen	25.05.2018

Titel	Gültig ab
§ 67 - Unterscheidung zwischen verschiedenen Kategorien betroffener Personen	25.05.2018
§ 68 - Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen	25.05.2018
§ 69 - Qualitätssicherung personenbezogener Daten vor deren Übermittlung	25.05.2018
§ 70 - Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung	25.05.2018
§ 71 - Protokollierung	25.05.2018
§ 72 - Vertrauliche Meldung von Verstößen	25.05.2018
Fünfter Abschnitt - Datenübermittlungen an Drittländer und an internationale Organisationen	25.05.2018
§ 73 - Allgemeine Voraussetzungen	25.05.2018
§ 74 - Datenübermittlung bei geeigneten Garantien	25.05.2018
§ 75 - Ausnahmen für eine Datenübermittlung ohne geeignete Garantien	25.05.2018
§ 76 - Sonstige Datenübermittlung an Empfänger in Drittländern	25.05.2018
Sechster Abschnitt - Zusammenarbeit der Aufsichtsbehörden	25.05.2018
§ 77 - Gegenseitige Amtshilfe	25.05.2018
Siebter Abschnitt - Haftung und Sanktionen	25.05.2018
§ 78 - Schadensersatz und Entschädigung	25.05.2018
§ 79 - Strafvorschriften	25.05.2018
VIERTER TEIL - Informationsfreiheit	25.05.2018
§ 80 - Anspruch auf Informationszugang	25.05.2018
§ 81 - Anwendungsbereich	24.11.2021
§ 82 - Schutz besonderer öffentlicher und privater Belange	25.05.2018
§ 83 - Schutz personenbezogener Daten	25.05.2018
§ 84 - Schutz behördlicher Entscheidungsprozesse	25.05.2018
§ 85 - Antrag	25.05.2018
§ 86 - Verfahren bei Beteiligung Dritter	25.05.2018
§ 87 - Entscheidung	25.05.2018
§ 88 - Kosten	24.11.2021
§ 89 - Die oder der Hessische Informationsfreiheitsbeauftragte	25.05.2018
FÜNFTER TEIL - Übergangs- und Schlussvorschriften	25.05.2018
§ 90 - Übergangsvorschriften	25.05.2018
§ 91 - Inkrafttreten	25.05.2018

Titel**Gültig ab**

Anlage: - Verwaltungskostenverzeichnis

25.05.2018

INHALTSVERZEICHNIS

ERSTER TEIL

Gemeinsame Bestimmungen

Erster Abschnitt

Anwendungsbereich und Begriffsbestimmungen

§ 1 Anwendungsbereich

§ 2 Begriffsbestimmungen

Zweiter Abschnitt

Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

§ 3 Verarbeitung personenbezogener Daten, Auftragsverarbeitung

§ 4 Videoüberwachung öffentlich zugänglicher Räume

Dritter Abschnitt

Datenschutzbeauftragte öffentlicher Stellen

§ 5 Benennung

§ 6 Rechtsstellung

§ 7 Aufgaben

Vierter Abschnitt

Die oder der Hessische Datenschutzbeauftragte

§ 8 Rechtsstellung und Unabhängigkeit

§ 9 Wahl

§ 10 Persönliche Voraussetzungen

§ 11 Amtsverhältnis

§ 12 Verschwiegenheitspflicht

§ 13 Zuständigkeit und Aufgaben

§ 14 Befugnisse

§ 15 Gutachten und Untersuchungen, Tätigkeitsbericht

§ 16 Informationspflichten

§ 17 Benachteiligungsverbot bei Anrufung der oder des Hessischen Datenschutzbeauftragten

§ 18 Personal- und Sachausstattung

Fünfter Abschnitt

Rechtsbehelfe

§ 19 Gerichtlicher Rechtsschutz

ZWEITER TEIL

Durchführungsbestimmungen für Verarbeitungen zu Zwecken nach Artikel 2 der Verordnung (EU) Nr. 2016/679

Erster Abschnitt

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Erster Titel

Verarbeitung personenbezogener Daten und Verarbeitung zu anderen Zwecken

§ 20 Verarbeitung besonderer Kategorien personenbezogener Daten

§ 21 Verarbeitung zu anderen Zwecken

§ 22 Datenübermittlungen durch öffentliche Stellen

Zweiter Titel

Besondere Verarbeitungssituationen

- § 23 Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses
- § 24 Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken
- § 25 Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken
- § 26 Rechte der betroffenen Person und aufsichtsbehördliche Untersuchungen im Fall von Geheimhaltungspflichten
- § 27 Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften
- § 28 Datenverarbeitung des Hessischen Rundfunks zu journalistischen Zwecken
- § 28a Datenverarbeitung bei öffentlichen Auszeichnungen und Ehrungen
- § 28b Datenverarbeitung in Gnadungsverfahren
- § 28c Datenübermittlung durch berufsständische Versorgungseinrichtungen

Dritter Titel

Rechte des Landtags und der kommunalen Vertretungsorgane

- § 29 Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane
- § 30 Verarbeitung personenbezogener Daten durch den Landtag und die kommunalen Vertretungsorgane

Zweiter Abschnitt

Rechte der betroffenen Person

- § 31 Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person
- § 32 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
- § 33 Auskunftsrecht der betroffenen Person
- § 34 Recht auf Löschung („Recht auf Vergessenwerden“)
- § 35 Widerspruchsrecht

Dritter Abschnitt

Sanktionen

- § 36 Anwendung der Vorschriften über das Bußgeld- und Strafverfahren bei Verstößen nach Artikel 83 der Verordnung (EU) Nr. 2016/679
- § 37 Strafvorschriften
- § 38 Bußgeldvorschriften

Vierter Abschnitt

Gemeinsame Verfahren, Gemeinsam Verantwortliche

- § 39 Gemeinsame Verfahren, Gemeinsam Verantwortliche

DRITTER TEIL

Bestimmungen für Verarbeitungen zu Zwecken nach Artikel 1 Absatz 1 der Richtlinie (EU) Nr. 2016/680

Erster Abschnitt

Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

- § 40 Anwendungsbereich
- § 41 Begriffsbestimmungen
- § 42 Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Zweiter Abschnitt

Rechtsgrundlagen für die Verarbeitung personenbezogener Daten

- § 43 Verarbeitung besonderer Kategorien personenbezogener Daten
- § 44 Verarbeitung zu anderen Zwecken
- § 45 Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken, archivarischen oder statistischen Zwecken
- § 46 Einwilligung
- § 47 Verarbeitung auf Weisung des Verantwortlichen
- § 48 Datengeheimnis
- § 49 Automatisierte Einzelentscheidung

Dritter Abschnitt

Rechte der betroffenen Person

- § 50 Allgemeine Informationen zu Datenverarbeitungen
- § 51 Benachrichtigung betroffener Personen
- § 52 Auskunftsrecht
- § 53 Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung
- § 54 Verfahren für die Ausübung der Rechte der betroffenen Person
- § 55 Anrufung der oder des Hessischen Datenschutzbeauftragten
- § 56 Rechtsschutz gegen Entscheidungen der oder des Hessischen Datenschutzbeauftragten oder bei deren oder dessen Untätigkeit

Vierter Abschnitt

Pflichten der Verantwortlichen und Auftragsverarbeiter

- § 57 Auftragsverarbeitung
- § 58 Gemeinsame Verfahren, Gemeinsam Verantwortliche
- § 59 Anforderungen an die Sicherheit der Datenverarbeitung
- § 60 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten
- § 61 Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten
- § 62 Durchführung einer Datenschutz-Folgenabschätzung
- § 63 Zusammenarbeit mit der oder dem Hessischen Datenschutzbeauftragten
- § 64 Vorherige Konsultation der oder des Hessischen Datenschutzbeauftragten
- § 65 Verzeichnis von Verarbeitungstätigkeiten
- § 66 Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- § 67 Unterscheidung zwischen verschiedenen Kategorien betroffener Personen
- § 68 Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen
- § 69 Qualitätssicherung personenbezogener Daten vor deren Übermittlung
- § 70 Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung
- § 71 Protokollierung
- § 72 Vertrauliche Meldung von Verstößen

Fünfter Abschnitt

Datenübermittlungen an Drittländer und an internationale Organisationen

- § 73 Allgemeine Voraussetzungen
- § 74 Datenübermittlung bei geeigneten Garantien
- § 75 Ausnahmen für eine Datenübermittlung ohne geeignete Garantien
- § 76 Sonstige Datenübermittlung an Empfänger in Drittländern

Sechster Abschnitt

Zusammenarbeit der Aufsichtsbehörden

§ 77 Gegenseitige Amtshilfe

Siebter Abschnitt

Haftung und Sanktionen

§ 78 Schadensersatz und Entschädigung

§ 79 Strafvorschriften

VIERTER TEIL

Informationsfreiheit

§ 80 Anspruch auf Informationszugang

§ 81 Anwendungsbereich

§ 82 Schutz besonderer öffentlicher und privater Belange

§ 83 Schutz personenbezogener Daten

§ 84 Schutz behördlicher Entscheidungsprozesse

§ 85 Antrag

§ 86 Verfahren bei Beteiligung Dritter

§ 87 Entscheidung

§ 88 Kosten

§ 89 Die oder der Hessische Informationsfreiheitsbeauftragte

FÜNFTER TEIL

Übergangs- und Schlussvorschriften

§ 90 Übergangsvorschriften

§ 91 Inkrafttreten

Anlage Verwaltungskostenverzeichnis

ERSTER TEIL

Gemeinsame Bestimmungen

Erster Abschnitt

Anwendungsbereich und Begriffsbestimmungen

§ 1

Anwendungsbereich

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch die öffentlichen Stellen des Landes, der Gemeinden und Landkreise.

(2) Andere Rechtsvorschriften über den Datenschutz gehen vorbehaltlich des Abs. 3 den Vorschriften dieses Gesetzes vor. Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes Anwendung. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(3) Die Vorschriften dieses Gesetzes gehen denen des Hessischen Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(4) Die Vorschriften dieses Gesetzes, ausgenommen § 28, finden keine Anwendung, soweit der Hessische Rundfunk personenbezogene Daten zu journalistischen Zwecken verarbeitet.

(5) Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, insbesondere die Verordnung (EU) Nr. 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, Nr. L 314 S. 72) in der jeweils geltenden Fassung, unmittelbar gilt.

(6) Bei Verarbeitungen zu den in Art. 2 der Verordnung (EU) Nr. 2016/679 genannten Zwecken stehen die Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum und die Schweiz den Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittländer.

(7) Bei Verarbeitungen zu den in Art. 1 Abs. 1 der Richtlinie (EU) Nr. 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. L 119 S. 89) genannten Zwecken stehen die bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes assoziierten Staaten den Mitgliedstaaten der Europäischen Union gleich. Andere Staaten gelten insoweit als Drittländer.

(8) Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten, die nicht in den Anwendungsbereich der Verordnung (EU) Nr. 2016/679 und der Richtlinie (EU) Nr. 2016/680 fallen, finden die Verordnung (EU) Nr. 2016/679 sowie der Erste und Zweite Teil entsprechende Anwendung, soweit gesetzlich nichts anderes bestimmt ist.

(9) Die Vorschriften dieses Gesetzes finden keine Anwendung auf anonyme Informationen oder anonymisierte Daten.

§ 2

Begriffsbestimmungen

(1) Öffentliche Stellen sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Landes, der Gemeinden und Landkreise oder sonstige deren Aufsicht unterstehende juristische Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Nimmt eine nicht öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

(2) Öffentliche Stellen gelten als nicht öffentliche Stellen, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Insoweit finden die für nicht öffentliche Stellen geltenden Vorschriften des Bundesdatenschutzgesetzes und die §§ 5 bis 18 und 23 Anwendung.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht öffentlicher Stellen als öffentliche Stellen, wenn einer oder mehreren öffentlichen Stellen die absolute Mehrheit der Anteile gehört oder der Stimmen zusteht. Beteiligt sich eine Vereinigung des privaten Rechts, die nach Satz 1 als öffentliche Stelle gilt, an einer weiteren Vereinigung des privaten Rechts, so finden Satz 1 und Abs. 2 entsprechende Anwendung.

(4) Anonyme Informationen sind solche Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann, sind anonymisierte Daten. Eine natürliche Person ist identifizierbar, wenn sie unter Berücksichtigung aller Mittel, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die Identität der natürlichen Person direkt oder indirekt zu ermitteln, identifiziert werden kann. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, insbesondere

die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.

Zweiter Abschnitt **Rechtsgrundlagen für die Verarbeitung personenbezogener Daten**

§ 3

Verarbeitung personenbezogener Daten, Auftragsverarbeitung

(1) Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

(2) Als Auftragsverarbeiter gelten auch Personen und Stellen, die im Auftrag Wartungsarbeiten und vergleichbare Hilfstätigkeiten bei der Verarbeitung personenbezogener Daten erledigen.

§ 4

Videoüberwachung öffentlich zugänglicher Räume

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung sowie der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

(3) Die Speicherung oder Verwendung von nach Abs. 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten und nicht geringfügigen Ordnungswidrigkeiten erforderlich ist.

(4) Die Daten sind zu löschen, sobald sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder wenn schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Dritter Abschnitt **Datenschutzbeauftragte öffentlicher Stellen**

§ 5

Benennung

(1) Öffentliche Stellen benennen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten sowie deren oder dessen Vertreterin oder Vertreter.

(2) Für mehrere öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer 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 § 7 genannten Aufgaben.

(4) Die oder der Datenschutzbeauftragte kann Beschäftigte oder Beschäftigter der öffentlichen Stelle sein 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 Hessischen Datenschutzbeauftragten mit.

§ 6 Rechtsstellung

(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 nach § 7, 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. Insbesondere ist die oder der Datenschutzbeauftragte im erforderlichen Umfang von der Erfüllung anderer Aufgaben freizustellen.

(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 untersteht und 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) Beschäftigte der öffentlichen Stellen können sich ohne Einhaltung des Dienstwegs in allen Angelegenheiten des Datenschutzes an die oder den Datenschutzbeauftragten wenden. Betroffene Personen können die Datenschutzbeauftragte oder den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte nach der Verordnung (EU) Nr. 2016/679, diesem Gesetz sowie anderen Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. Die oder der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person verpflichtet, die ihr oder ihm in der Eigenschaft als Datenschutzbeauftragte oder Datenschutzbeauftragter Tatsachen anvertraut hat. Die Verschwiegenheitspflicht erstreckt sich auch auf die Umstände, die Rückschlüsse auf die betroffene Person zulassen, sowie auf diese Tatsachen selbst, soweit die oder der Datenschutzbeauftragte nicht durch die betroffene Person davon befreit wird.

(5) 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 Beschäftigten 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. So weit das Zeugnisverweigerungsrecht der oder des Datenschutzbeauftragten reicht, unterliegen ihre oder seine Akten und andere Dokumente einem Beschlagnahmeverbot.

§ 7 Aufgaben

(1) Der oder dem Datenschutzbeauftragten obliegen neben den in der Verordnung (EU) Nr. 2016/679 genannten Aufgaben zumindest folgende Aufgaben:

1. Unterrichtung und Beratung der öffentlichen Stelle und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften,
2. Überwachung der Einhaltung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 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 Beschäftigten und der diesbezüglichen Überprüfungen,
3. Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung nach § 62,
4. Zusammenarbeit mit der oder dem Hessischen Datenschutzbeauftragten,
5. Tätigkeit als Anlaufstelle für die oder den Hessischen Datenschutzbeauftragten in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation nach § 64, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Im Fall 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 und Pflichten 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.

Vierter Abschnitt Die oder der Hessische Datenschutzbeauftragte

§ 8 Rechtsstellung und Unabhängigkeit

(1) Die oder der Hessische Datenschutzbeauftragte ist eine oberste Landesbehörde.

(2) Die oder der Hessische Datenschutzbeauftragte handelt in Ausübung ihres oder seines Amtes unabhängig und ist nur dem Gesetz unterworfen. Sie oder er unterliegt bei der Erfüllung ihrer oder seiner Aufgaben und bei der Ausübung ihrer oder seiner Befugnisse weder direkter noch indirekter Beeinflussung von außen und ersucht weder um Weisung noch nimmt sie oder er Weisungen entgegen.

(3) Die oder der Hessische Datenschutzbeauftragte unterliegt der Rechnungsprüfung durch den Hessischen Rechnungshof.

(4) Die oder der Hessische Datenschutzbeauftragte ist berechtigt, an den Sitzungen des Landtags und seiner Ausschüsse nach Maßgabe der Geschäftsordnung des Landtags teilzunehmen und sich zu Fragen zu äußern, die für den Datenschutz von Bedeutung sind. Der Landtag und seine Ausschüsse können die Anwesenheit der oder des Hessischen Datenschutzbeauftragten verlangen.

§ 9

Wahl

(1) Der Landtag wählt auf Vorschlag der Landesregierung die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten.

(2) Die Präsidentin oder der Präsident des Landtags verpflichtet die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten vor dem Landtag, ihr oder sein Amt gerecht und unparteiisch zu führen und die Verfassung des Landes Hessen und das Grundgesetz für die Bundesrepublik Deutschland und die Gesetze getreulich zu wahren.

§ 10

Persönliche Voraussetzungen

Die oder der Hessische Datenschutzbeauftragte muss über die für die Erfüllung ihrer oder seiner Aufgaben und die Ausübung ihrer oder seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen und die Befähigung zum Richteramt oder zum höheren Dienst haben.

§ 11

Amtsverhältnis

(1) Die oder der Hessische Datenschutzbeauftragte steht nach Maßgabe dieses Gesetzes zum Land in einem öffentlich-rechtlichen Amtsverhältnis. Sie oder er übt ihre oder seine Tätigkeit hauptamtlich aus. Die oder der Hessische Datenschutzbeauftragte sieht von allen mit den Aufgaben ihres oder seines Amtes nicht zu vereinbarenden Handlungen ab und übt während der Amtszeit keine mit dem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus. Die oder der Hessische Datenschutzbeauftragte erteilt dem Landtag jährlich Auskunft über Art und Umfang der von ihr oder ihm im Kalenderjahr ausgeübten Nebentätigkeiten sowie über die dafür erhaltenen Vergütungen.

(2) Die oder der Hessische Datenschutzbeauftragte wird für die Dauer von fünf Jahren gewählt. Das Amtsverhältnis endet mit Ablauf der Amtszeit oder mit dem Rücktritt. Die oder der Hessische Datenschutzbeauftragte bleibt bis zur Neuwahl im Amt. Die Wiederwahl ist zulässig. Durch Urteil des Staatsgerichtshofs können ihr oder ihm das Amt und die Rechte aus dem Amt abgesprochen werden, wenn Tatsachen vorliegen, die bei einer Beamtin oder einem Beamten die Entlassung nach den §§ 22 und 23 Abs. 1 und 3 Nr. 1 des Beamtenstatusgesetzes vom 17. Juni 2008 (BGBl. I S. 1010), zuletzt geändert durch Gesetz vom 8. Juni 2017 (BGBl. I S. 1570), oder die Beendigung des Dienstverhältnisses nach § 24 des Beamtenstatusgesetzes rechtfertigen. Der Antrag auf Erhebung der Klage muss von

mindestens 15 Mitgliedern des Landtags unterzeichnet sein und bedarf der Zustimmung von zwei Dritteln der gesetzlichen Zahl seiner Mitglieder. Die §§ 31 bis 35 des Gesetzes über den Staatsgerichtshof in der Fassung der Bekanntmachung vom 19. Januar 2001 (GVBl. I S. 78), zuletzt geändert durch Gesetz vom 28. März 2015 (GVBl. S. 158), sind entsprechend anzuwenden.

(3) Die oder der Hessische Datenschutzbeauftragte kann jederzeit von ihrem oder seinem Amt zurücktreten.

(4) Die oder der Hessische Datenschutzbeauftragte ernennt für den Fall der Verhinderung oder des vorzeitigen Ausscheidens aus dem Amt für die Zeit bis zur Wahl einer oder eines neuen Hessischen Datenschutzbeauftragten eine Beschäftigte oder einen Beschäftigten ihrer oder seiner Dienststelle zur Vertreterin oder zum Vertreter. Als Verhinderung gilt auch, wenn im Einzelfall in der Person der oder des Hessischen Datenschutzbeauftragten Gründe vorliegen, die bei einer Richterin oder einem Richter zum Ausschluss von der Mitwirkung oder zur Ablehnung wegen Besorgnis der Befangenheit führen können.

(5) Die oder der Hessische Datenschutzbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Ende des Kalendermonats, in dem das Amtsverhältnis endet, als Amtsbezüge ein Amtsgehalt in Höhe des Grundgehalts der Besoldungsgruppe B 7 sowie einen Familienzuschlag in entsprechender Anwendung des Hessischen Besoldungsgesetzes vom 27. Mai 2013 (GVBl. S. 218, 256, 508), zuletzt geändert durch Gesetz vom 30. Juni 2017 (GVBl. S. 114), in der jeweils geltenden Fassung. Für Reise- und Umzugskosten, Trennungsgeld, Beihilfen und Urlaubsangelegenheiten der oder des Hessischen Datenschutzbeauftragten gelten die für die Beamtinnen und Beamten des Landes geltenden Vorschriften entsprechend.

(6) Zuständig für die Festsetzung, Berechnung und Anordnung der Zahlung der Amtsbezüge einschließlich der Sonderzahlungen sowie der Rückforderung zu viel gezahlter Amtsbezüge ist die Hessische Bezügestelle im Auftrag der oder des Hessischen Datenschutzbeauftragten. Zuständig für die Festsetzung von Reise- und Umzugskosten sowie Trennungsgeld ist die Dienststelle der oder des Hessischen Datenschutzbeauftragten. Zuständig für die Festsetzung der Beihilfe ist die Kanzlei des Hessischen Landtags.

(7) Die oder der Hessische Datenschutzbeauftragte und deren oder dessen Hinterbliebene erhalten Versorgung in entsprechender Anwendung der in Hessen für die Mitglieder der Landesregierung geltenden Bestimmungen. Zuständig für die Festsetzung der Versorgungsbezüge ist das Regierungspräsidium Kassel im Auftrag der oder des Hessischen Datenschutzbeauftragten.

§ 12

Verschwiegenheitspflicht

Die oder der Hessische Datenschutzbeauftragte ist, auch nach Beendigung ihres oder seines Amtsverhältnisses, verpflichtet, über die ihr oder ihm bei ihrer oder seiner amtlichen Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Satz 1 und 2 gelten entsprechend für ihre oder seine Beschäftigten. Die oder der Hessische Datenschutzbeauftragte gilt als oberste Dienstbehörde im Sinne des § 96 der Strafprozessordnung. Sie oder er entscheidet entsprechend den Bestimmungen über die Vorlage- und Auskunftspflichten von Behörden in den gerichtlichen Verfahrensordnungen. Die oder der Hessische Datenschutzbeauftragte trifft die Entscheidungen nach § 37 Abs. 3 des Beamtenstatusgesetzes und § 46 des Hessischen Beamtengesetzes für sich und die bei ihr oder ihm tätigen Beamtinnen und Beamten.

§ 13

Zuständigkeit und Aufgaben

(1) Die oder der Hessische Datenschutzbeauftragte überwacht bei den öffentlichen und nicht öffentlichen Stellen sowie deren Auftragsverarbeitern die Anwendung dieses Gesetzes, der Verordnung (EU) Nr. 2016/679 und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften.

(2) Neben den Aufgaben nach Art. 57 der Verordnung (EU) Nr. 2016/679 hat die oder der Hessische Datenschutzbeauftragte die Aufgaben,

1. die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 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 sie darüber aufzuklären, wobei spezifische Maßnahmen für Kinder und Jugendliche besondere Beachtung finden,
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 aus diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, entstehenden Pflichten bei der Verarbeitung personenbezogener Daten zu sensibilisieren,
5. auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 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 Beschwerden einer Stelle, einer Organisation oder eines Verbandes nach Art. 55 der Richtlinie (EU) Nr. 2016/680 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 dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 2016/680 erlassenen Rechtsvorschriften, zu gewährleisten,
8. Untersuchungen über die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) Nr. 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 und
10. Beratung in Bezug auf die in § 64 genannten Verarbeitungsvorgänge zu leisten.

Im Anwendungsbereich der Richtlinie (EU) Nr. 2016/680 nimmt die oder der Hessische Datenschutzbeauftragte zudem die Aufgaben nach § 52 Abs. 7 auch in Verbindung mit § 51 Abs. 4, § 53 Abs. 7 und § 55 wahr.

(3) Die oder der Hessische Datenschutzbeauftragte beobachtet die Auswirkungen der automatisierten Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der öffentlichen Stellen, insbesondere ob diese zu einer Verschiebung in der Gewaltenteilung zwischen den Verfassungsorganen des Landes, zwischen den Organen der kommunalen Selbstverwaltung oder zwischen der staatlichen Verwaltung und der kommunalen Selbstverwaltung führen. Sie oder er soll Maßnahmen anregen, die geeignet erscheinen, derartige Auswirkungen zu verhindern.

(4) Die oder der Hessische Datenschutzbeauftragte ist

1. zuständige Behörde für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach
 - a) § 38 und
 - b) Art. 83 Abs. 4 bis 6 der Verordnung (EU) Nr. 2016/679 sowie
2. zuständige Stelle für die Leistung von Hilfe nach Art. 13 Abs. 2 Buchst. a des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 (BGBl. 1985 II S. 538, 539).

(5) Abs. 2 Satz 1 Nr. 1 gilt nicht für das Handeln der Gerichte im Rahmen ihrer justiziellen Tätigkeit.

(6) Zur Erfüllung der in Abs. 2 Satz 1 Nr. 3 genannten Aufgabe kann die oder der Hessische Datenschutzbeauftragte von sich aus oder auf Anfrage Stellungnahmen an den Landtag oder einen seiner Ausschüsse, die Landesregierung, die Kommunen, sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit richten. Auf Ersuchen des Landtags oder eines seiner Ausschüsse, der Landesregierung, der Kommunen, sonstiger Einrichtungen und Stellen geht die oder der Hessische Datenschutzbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes nach.

(7) Die oder der Hessische Datenschutzbeauftragte erleichtert das Einreichen der in Abs. 2 Satz 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.

(8) Zur Erfüllung der in Abs. 2 Satz 1 Nr. 7 genannten Aufgabe kann die oder der Hessische Datenschutzbeauftragte anderen Aufsichtsbehörden Informationen übermitteln und ihnen Amtshilfe leisten.

(9) Für die Erfüllung der Aufgaben und Gewährung der Auskunft nach § 80 Abs. 1 erhebt die oder der Hessische Datenschutzbeauftragte Kosten (Gebühren und Auslagen) nach Maßgabe des Hessischen Verwaltungskostengesetzes in der Fassung der Bekanntmachung vom 12. Januar 2004 (GVBl. I S. 36), zuletzt geändert durch Gesetz vom 13. Dezember 2012 (GVBl. S. 622), und § 88 Abs. 1 in Verbindung mit der Anlage zu diesem Gesetz.

(10) Die Erfüllung der Aufgaben der oder des Hessischen Datenschutzbeauftragten ist für die betroffene Person verwaltungskostenfrei. Bei offenkundig unbegründeten oder, insbesondere im Fall von häufiger Wiederholung, exzessiven Anfragen kann die oder der Hessische Datenschutzbeauftragte eine Gebühr auf der Grundlage der Anlage zu diesem Gesetz verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die oder der Hessische Datenschutzbeauftragte die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

(11) Die Landesregierung wird ermächtigt, nach Anhörung der oder des Hessischen Datenschutzbeauftragten die Anlage zu diesem Gesetz durch Rechtsverordnung nach Maßgabe des Hessischen Verwaltungskostengesetzes zu ändern.

§ 14 Befugnisse

(1) Die oder der Hessische Datenschutzbeauftragte nimmt im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 die Befugnisse nach Art. 58 der Verordnung (EU) Nr. 2016/679 wahr. Kommt die oder der Hessische Datenschutzbeauftragte zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt sie oder er dies der öffentlichen Stelle mit und gibt dieser vor der Ausübung der Befugnisse des Art. 58 Abs. 2 Buchst. b bis g, i und j der Verordnung (EU) Nr. 2016/679 Gelegenheit zur Stellungnahme innerhalb einer angemessenen Frist. Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilung der oder des Hessischen Datenschutzbeauftragten getroffen worden sind. Die Ausübung der Befugnisse nach Art. 58 Abs. 2 Buchst. b bis g, i und j der Verordnung (EU) Nr. 2016/679 teilt die oder der Hessische Datenschutzbeauftragte der jeweils zuständigen Rechts- und Fachaufsichtsbehörde mit.

(2) Stellt die oder der Hessische Datenschutzbeauftragte bei Datenverarbeitungen zu Zwecken außerhalb des Anwendungsbereichs der Verordnung (EU) Nr. 2016/679 Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie oder er dies im Fall einer öffentlichen Stelle

1. des Landes gegenüber der zuständigen obersten Landesbehörde,
2. einer Gemeinde oder eines Landkreises gegenüber dem jeweiligen vertretungsberechtigten Organ

und fordert diese zur Stellungnahme innerhalb einer von ihr oder ihm zu bestimmenden Frist auf. In den Fällen des Satz 1 Nr. 2 unterrichtet die oder der Hessische Datenschutzbeauftragte gleichzeitig die zuständige Aufsichtsbehörde. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung der oder des Hessischen Datenschutzbeauftragten getroffen worden sind. Die oder der Hessische Datenschutzbeauftragte kann von einer Beanstandung absehen

oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die oder der Hessische Datenschutzbeauftragte 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.

(3) Die oder der Hessische Datenschutzbeauftragte kann bei Verstößen nach Abs. 2 Satz 1 darüber hinaus anordnen,

1. Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise oder innerhalb eines bestimmten Zeitraums, mit den Vorschriften 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.

(4) Die öffentlichen Stellen sind verpflichtet, die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Ihr oder ihm ist 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,
3. Zugang zu den Grundstücken und Diensträumen einschließlich aller Datenverarbeitungsanlagen und -geräte zu gewähren,

soweit dies zur Erfüllung ihrer oder seiner Aufgaben erforderlich ist.

(5) Wenn eine oberste Landesbehörde im Einzelfall feststellt, dass die Sicherheit des Bundes oder eines Landes dies gebietet, dürfen die Rechte nach Abs. 3 nur von der oder dem Hessischen Datenschutzbeauftragten persönlich ausgeübt werden. In diesem Fall dürfen personenbezogene Daten einer betroffenen Person, der von dem Verantwortlichen Vertraulichkeit besonders zugesichert worden ist, auch der oder dem Hessischen Datenschutzbeauftragten gegenüber nicht offenbart werden.

§ 15

Gutachten und Untersuchungen, Tätigkeitsbericht

(1) Der Landtag und die Landesregierung können die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten mit der Erstattung von Gutachten und der Durchführung von Untersuchungen in Datenschutzfragen und Fragen des freien Zugangs zu Informationen betrauen.

(2) Der Landtag, die Präsidentin oder der Präsident des Landtags und die in § 29 Abs. 3 genannten Vertretungsorgane können verlangen, dass die oder der Hessische Datenschutzbeauftragte untersucht, aus welchen Gründen Auskunftersuchen nicht oder nicht ausreichend beantwortet wurden.

(3) Zum 31. Dezember jedes Jahres hat die oder der Hessische Datenschutzbeauftragte dem Landtag und der Landesregierung einen Bericht über das Ergebnis ihrer oder seiner Tätigkeit vorzulegen und regt Verbesserungen des Datenschutzes an. Die oder der Hessische Datenschutzbeauftragte macht diesen Bericht der Öffentlichkeit, der Europäischen Kommission und dem Europäischen Datenschutzausschuss zugänglich. Zwischenberichte zur Vorlage bei dem Landtag und der Landesregierung sind zulässig.

(4) Die Landesregierung legt ihre Stellungnahme zu einem Bericht nach Abs. 3 Satz 1 oder 3, soweit dessen Gegenstand die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist, dem Landtag vor.

§ 16

Informationspflichten

(1) Die oder der Hessische Datenschutzbeauftragte ist über Verfahrensentwicklungen im Zusammenhang mit der automatisierten Verarbeitung personenbezogener Daten rechtzeitig und umfassend zu unterrichten.

(2) Wird die oder der Hessische Datenschutzbeauftragte aufgrund einer Rechtsvorschrift gehört, soll sie oder er unverzüglich mitteilen, ob und innerhalb welcher Frist eine Stellungnahme abgegeben wird.

§ 17

Benachteiligungsverbot bei Anrufung der oder des Hessischen Datenschutzbeauftragten

Unbeschadet des Art. 77 der Verordnung (EU) Nr. 2016/679 sowie § 55 darf keiner Person ein Nachteil daraus erwachsen, dass sie sich aufgrund tatsächlicher Anhaltspunkte für einen Verstoß gegen Vorschriften dieses Gesetzes oder anderer Vorschriften über den Datenschutz an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wendet. Beschäftigte öffentlicher Stellen können sich ohne Einhaltung des Dienstwegs an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wenden. Die dienstrechtlichen Pflichten der Beschäftigten bleiben im Übrigen unberührt.

§ 18

Personal- und Sachausstattung

(1) Der oder dem Hessischen Datenschutzbeauftragten ist die für die Erfüllung ihrer oder seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen. Sie ist im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen. Die Präsidentin oder der Präsident des Landtags nimmt die Personal- und Sachausstattung nach Auswahl der oder des Hessischen Datenschutzbeauftragten vor.

(2) Die Beamtinnen und Beamten werden von der oder dem Hessischen Datenschutzbeauftragten ausgewählt und auf deren oder dessen Vorschlag durch die Präsidentin oder den Präsidenten des Landtags ernannt. Ihre Dienstvorgesetzte oder ihr Dienstvorgesetzter ist die oder der Hessische Datenschutzbeauftragte, an deren oder dessen Weisungen sie ausschließlich gebunden sind. Die oder

der Hessische Datenschutzbeauftragte übt für die bei ihr oder ihm tätigen Beamtinnen und Beamten die Aufgaben der obersten Dienstbehörde nach dem Hessischen Disziplinalgesetz aus. Für sonstige Beschäftigte gelten Satz 1 und 2 entsprechend.

Fünfter Abschnitt Rechtsbehelfe

§ 19

Gerichtlicher Rechtsschutz

- (1) Für Streitigkeiten zwischen einer natürlichen oder einer juristischen Person und der oder dem Hessischen Datenschutzbeauftragten über Rechte nach Art. 78 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679 sowie § 56 ist der Verwaltungsrechtsweg gegeben. Satz 1 gilt nicht für Bußgeldverfahren.
- (2) Für Verfahren nach Abs. 1 Satz 1 findet § 20 Abs. 2, 3, 5 und 7 des Bundesdatenschutzgesetzes entsprechende Anwendung.
- (3) In Verfahren nach Abs. 1 Satz 1 ist die oder der Hessische Datenschutzbeauftragte beteiligungsfähig.
- (4) Für Klagen betroffener Personen gegen einen Verantwortlichen oder einen Auftragsverarbeiter wegen eines Verstoßes gegen datenschutzrechtliche Bestimmungen im Anwendungsbereich der Verordnung (EU) Nr. 2016/679 oder der darin enthaltenen Rechte der betroffenen Person findet § 44 des Bundesdatenschutzgesetzes entsprechende Anwendung.
- (5) Behörden und sonstige öffentliche Stellen des Landes können unbeschadet anderer Rechtsbehelfe gerichtlich gegen sie betreffende verbindliche Entscheidungen der oder des Hessischen Datenschutzbeauftragten vorgehen. Wenn die Behörde oder öffentliche Stelle eine verbindliche Entscheidung der oder des Hessischen Datenschutzbeauftragten nicht beachtet und nicht innerhalb eines Monats nach Bekanntgabe gerichtlich gegen diese vorgeht, kann die oder der Hessische Datenschutzbeauftragte die gerichtliche Feststellung der Rechtmäßigkeit der getroffenen verbindlichen Entscheidung beantragen.
- (6) Die Klage einer Behörde oder sonstigen öffentlichen Stelle des Landes gegen eine verbindliche Entscheidung der oder des Hessischen Datenschutzbeauftragten nach Art. 58 Abs. 2 Buchst. g der Verordnung (EU) Nr. 2016/679 oder § 14 Abs. 3 Nr. 4 hat aufschiebende Wirkung.

ZWEITER TEIL

Durchführungsbestimmungen für Verarbeitungen zu Zwecken nach Artikel 2 der Verordnung (EU) Nr. 2016/679

Erster Abschnitt

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Erster Titel

Verarbeitung personenbezogener Daten und Verarbeitung zu anderen Zwecken

§ 20

Verarbeitung besonderer Kategorien personenbezogener Daten

- (1) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 durch öffentliche Stellen zulässig, wenn sie

1. erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen,
2. zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit der Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist, und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, oder
3. aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist; ergänzend zu den in Abs. 2 genannten Maßnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten,
4.
 - a) aus Gründen eines erheblichen öffentlichen Interesses unbedingt erforderlich ist,
 - b) zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist oder
 - c) aus zwingenden Gründen der Verteidigung oder für humanitäre Maßnahmen erforderlich ist

und soweit die Interessen des Verantwortlichen an der Datenverarbeitung die Interessen der betroffenen Person überwiegen.

(2) In den Fällen des Abs. 1 sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung nach der Verordnung (EU) Nr. 2016/679 erfolgt,
2. Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind,
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
4. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern,
5. Pseudonymisierung personenbezogener Daten,

6. Verschlüsselung personenbezogener Daten,
7. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
8. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen oder
9. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) Nr. 2016/679 sicherstellen.

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

§ 21

Verarbeitung zu anderen Zwecken

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn

1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,
2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
3. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder Ordnung, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- oder Zollaufkommens erforderlich ist,
4. sie zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbußen erforderlich ist,
5. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte und Freiheiten einer anderen Person erforderlich ist oder
6. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen des Abs. 1 und ein Ausnahmetatbestand nach Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 oder nach § 20 Abs. 1 vorliegen.

(3) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage verarbeitet werden, dürfen nicht für andere Zwecke verarbeitet werden.

§ 22

Datenübermittlungen durch öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 21 zulassen würden. Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist unter den Voraussetzungen des § 21 zulässig.

(2) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an nicht öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach § 21 zulassen würden,
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder
3. es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist

und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

(3) Die Übermittlung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist zulässig, wenn die Voraussetzungen des Abs. 1 oder 2 und ein Ausnahmetatbestand nach Art. 9 Abs. 2 der Verordnung (EU) Nr. 2016/679 oder nach § 20 Abs. 1 vorliegen.

(4) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Ist die Übermittlung zur Erfüllung von Aufgaben eines in § 2 Abs. 1 und 3 genannten Empfängers erforderlich, so trägt auch dieser hierfür die Verantwortung und hat sicherzustellen, dass die Erforderlichkeit nachträglich überprüft werden kann. Die übermittelnde Stelle hat in diesem Fall die Zuständigkeit des Empfängers und die Schlüssigkeit der Anfrage zu überprüfen. Bestehen im Einzelfall Zweifel an der Schlüssigkeit, so hat sie darüber hinaus die Erforderlichkeit zu überprüfen. Der Empfänger hat der übermittelnden Stelle die für ihre Prüfung erforderlichen Angaben zu machen.

Zweiter Titel

Besondere Verarbeitungssituationen

§ 23

Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung, Beendigung oder Abwicklung sowie zur Durchführung innerdienstlicher planerischer, organisatorischer, sozialer und personeller Maßnahmen erforderlich ist. Dies gilt auch zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im 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 Dienstherr oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Dienstherr oder Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 der Verordnung (EU) Nr. 2016/679 in Textform aufzuklären.

(3) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Abs. 2 gilt auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. § 20 Abs. 2 gilt entsprechend.

(4) Die Verarbeitung personenbezogener Daten einschließlich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Art. 88 Abs. 2 der Verordnung (EU) Nr. 2016/679 zu beachten.

(5) Der Verantwortliche muss geeignete Maßnahmen ergreifen, um sicherzustellen, dass insbesondere die in Art. 5 der Verordnung (EU) Nr. 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

(6) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

(7) Die Abs. 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschließlich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Die für das Personalaktenrecht geltenden Vorschriften des Hessischen Beamtengesetzes sind, soweit tarifvertraglich nichts Abweichendes geregelt ist, auf Arbeitnehmerinnen und Arbeitnehmer im öffentlichen Dienst entsprechend anzuwenden.

(8) Beschäftigte im Sinne dieses Gesetzes sind:

1. Arbeitnehmerinnen und Arbeitnehmer, einschließlich der Leiharbeiterinnen und Leiharbeiter im Verhältnis zum Entleiher,
2. zu ihrer Berufsausbildung Beschäftigte,
3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),
4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,
5. Freiwillige, die einen Dienst nach dem Jugendfreiwilligendienstegesetz vom 16. Mai 2008 (BGBl. I S. 842), geändert durch Gesetz vom 20. Dezember 2011 (BGBl. I S. 2854), oder dem Bundesfreiwilligendienstgesetz vom 28. April 2011 (BGBl. I S. 687), zuletzt geändert durch Gesetz vom 20. Oktober 2015 (BGBl. I S. 1722), leisten,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Beamtinnen und Beamte im Geltungsbereich des Hessischen Beamtengesetzes, Richterinnen und Richter des Landes sowie Zivildienstleistende.

Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.

§ 24

Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

(1) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person nach § 20 Abs. 2 Satz 2 vor. Vor dem Beginn des Forschungsvorhabens ist ein Datenschutzkonzept zu erstellen, das der zuständigen Aufsichtsbehörde auf Nachfrage vorzulegen ist.

(2) Die in den Art. 15, 16, 18 und 21 der Verordnung (EU) Nr. 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft nach Art. 15 der Verordnung (EU) Nr. 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu den in § 20 Abs. 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. Sobald der Forschungs- oder Statistikzweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungs- oder Statistikzweck dies zulässt.

(4) Der Verantwortliche darf personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 25

Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken

(1) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person nach § 20 Abs. 2 Satz 2 vor.

(2) Das Recht auf Auskunft der betroffenen Person nach Art. 15 der Verordnung (EU) Nr. 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

(3) Das Recht auf Berichtigung der betroffenen Person nach Art. 16 der Verordnung (EU) Nr. 2016/679 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

(4) Die in Art. 18 Abs. 1 Buchst. a, b und d, Art. 20 und 21 der Verordnung (EU) Nr. 2016/679 vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

§ 26

Rechte der betroffenen Person und auf sichtsbehördliche Untersuchungen im Fall von Geheimhaltungspflichten

(1) Die Pflicht zur Information der betroffenen Person nach Art. 14 Abs. 1 bis 4 der Verordnung (EU) Nr. 2016/679 besteht ergänzend zu den in Art. 14 Abs. 5 der Verordnung (EU) Nr. 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

(2) Das Recht auf Auskunft der betroffenen Person nach Art. 15 der Verordnung (EU) Nr. 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen.

(3) Die Pflicht zur Benachrichtigung nach Art. 34 der Verordnung (EU) Nr. 2016/679 besteht ergänzend zu der in Art. 34 Abs. 3 der Verordnung (EU) Nr. 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend von der Ausnahme nach Satz 1 ist die betroffene Person nach Art. 34 der Verordnung (EU) Nr. 2016/679 zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

(4) Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person nach Art. 13 Abs. 3 der Verordnung (EU) Nr. 2016/679 nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.

(5) Erlangt die oder der Hessische Datenschutzbeauftragte oder ihre oder seine Beschäftigten im Rahmen einer Untersuchung Kenntnis von Daten, die nach einer Rechtsvorschrift oder ihrem Wesen nach einer Geheimhaltungspflicht unterliegen, gilt diese auch für sie.

§ 27

Datenübermittlung an öffentlich-rechtliche Religionsgemeinschaften

Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgemeinschaften ist in entsprechender Anwendung der Vorschriften über die Übermittlung an öffentliche Stellen nur zulässig, sofern auf Grundlage geeigneter Garantien sichergestellt ist, dass bei der empfangenden Stelle eine Datenverarbeitung im Einklang mit der Verordnung (EU) Nr. 2016/679 erfolgt.

§ 28

Datenverarbeitung des Hessischen Rundfunks zu journalistischen Zwecken

(1) Führt die journalistische Verarbeitung personenbezogener Daten zur Veröffentlichung von Gegendarstellungen der betroffenen Personen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(2) Der Rundfunkrat bestellt eine Beauftragte oder einen Beauftragten für den Datenschutz, die oder der die Ausführung von Abs. 1 sowie anderer Vorschriften über den Datenschutz im journalistischen Bereich frei von Weisungen überwacht. An sie oder ihn kann sich jede Person wenden, wenn sie annimmt, bei der Verarbeitung personenbezogener Daten zu journalistischen Zwecken in ihren Rechten verletzt worden zu sein. Beanstandungen richtet die oder der Beauftragte für den Datenschutz an die

Intendantin oder den Intendanten und unterrichtet gleichzeitig den Rundfunkrat. Die Dienstaufsicht obliegt dem Verwaltungsrat.

(3) Der oder dem nach Abs. 2 zu bestellenden Beauftragten für den Datenschutz können auch die Aufgaben nach § 7 zugewiesen werden.

§ 28a

Datenverarbeitung bei öffentlichen Auszeichnungen und Ehrungen

(1) Die für die Vorbereitung und Durchführung öffentlicher Auszeichnungen und Ehrungen erforderlichen personenbezogenen Daten einschließlich der Daten nach Art. 9 Abs. 1 der Verordnung (EU) Nr. 2016/679 dürfen von

1. den zuständigen Stellen auch ohne Kenntnis der betroffenen Person verarbeitet werden,
2. anderen öffentlichen Stellen auch ohne Kenntnis der betroffenen Person an die dafür zuständigen Stellen übermittelt werden.

Soweit eine Verarbeitung ausschließlich für die in Satz 1 genannten Zwecke erfolgt, sind die Art. 13, 14, 16 und 19 bis 21 Abs. 4 der Verordnung (EU) Nr. 2016/679 nicht anzuwenden.

(2) Eine Verarbeitung der in Abs. 1 Satz 1 genannten Daten für andere als die dort genannten Zwecke ist nur mit Einwilligung der betroffenen Person zulässig.

§ 28b

Datenverarbeitung in Gnadenverfahren

(1) In Gnadenverfahren ist die Verarbeitung personenbezogener Daten einschließlich der Daten nach Art. 9 Abs. 1 und Art. 10 der Verordnung (EU) Nr. 2016/679 zulässig, soweit sie zur Ausübung des Gnadenrechts durch die zuständigen Stellen erforderlich ist.

(2) In Gnadenverfahren finden nur die Art. 4 und 5 sowie Kapitel IV mit Ausnahme von Art. 33 und 34 der Verordnung (EU) Nr. 2016/679 entsprechende Anwendung.

§ 28c

Datenübermittlung durch berufsständische Versorgungseinrichtungen

Verlangt eine Behörde, ein Vollstreckungsorgan oder ein Gericht aufgrund gesetzlicher Befugnis von einer berufsständischen Versorgungseinrichtung im Sinne des § 6 Abs. 1 Satz 1 Nr. 1 des Sechsten Buches Sozialgesetzbuch Auskunft über

1. die derzeitige Anschrift,
2. den derzeitigen oder zukünftigen Aufenthaltsort oder
3. den Namen und die Vornamen oder die Firma sowie die Anschrift des derzeitigen Arbeitgebers

eines Mitglieds dieser Versorgungseinrichtung, darf die Versorgungseinrichtung diese Daten an die Behörde, das Vollstreckungsorgan oder das Gericht übermitteln. Die Versorgungseinrichtung verwei-

gert die Auskunft, wenn sie Grund zu der Annahme hat, dass durch die Übermittlung schutzwürdige Interessen der betroffenen Person unangemessen beeinträchtigt werden.

Dritter Titel **Rechte des Landtags und der kommunalen Vertretungsorgane**

§ 29

Auskunftsrecht des Landtags und der kommunalen Vertretungsorgane

(1) Die Hessische Zentrale für Datenverarbeitung, die Kommunalen Gebietsrechenzentren und die öffentlichen Stellen des Landes, die Datenverarbeitungsanlagen und -geräte betreiben, sind verpflichtet, dem Landtag, der Präsidentin oder dem Präsidenten des Landtags und den Fraktionen des Landtags die von diesen im Rahmen ihrer Zuständigkeit verlangten Auskünfte aufgrund der gespeicherten Daten zu geben, soweit Programme zur Auswertung vorhanden sind. Die Auskünfte dürfen keine personenbezogenen Daten enthalten. Den Auskünften darf ein gesetzliches Verbot oder ein öffentliches Interesse nicht entgegenstehen. Dem Auskunftsrecht des Landtags steht ein öffentliches Interesse in der Regel nicht entgegen. Der Landtag hat Zugriff auf die Daten, soweit durch technische Maßnahmen sichergestellt ist, dass die Grenzen von Satz 1 bis 3 eingehalten werden.

(2) Der Landtag kann von der Landesregierung Auskünfte über die bestehenden Verfahren verlangen, die für Auskünfte oder den Zugriff nach Abs. 1 geeignet sind. Das Auskunftsverlangen kann sich erstrecken auf

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

(3) Das Auskunftsrecht nach Abs. 1 steht im Rahmen ihrer Zuständigkeiten den Gemeindevertretungen und den Kreistagen sowie deren Fraktionen und den entsprechenden Organen der anderen in § 2 Abs. 1 genannten öffentlichen Stellen gegenüber der Hessischen Zentrale für Datenverarbeitung, dem zuständigen Kommunalen Gebietsrechenzentrum und den Behörden der Gemeinden und Landkreise zu, die Datenverarbeitungsanlagen und -geräte betreiben. Anträge der Fraktionen sind in den Gemeinden über den Gemeindevorstand, in den Kreisen über den Kreisausschuss zu leiten.

§ 30

Verarbeitung personenbezogener Daten durch den Landtag und die kommunalen Vertretungsorgane

(1) Mit Ausnahme der §§ 15 und 29 gelten die Vorschriften dieses Gesetzes für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird, insbesondere wenn es sich um die wirtschaftlichen Angelegenheiten des Landtags, die Personalverwaltung oder die Ausführung von gesetzlichen Vorschriften, deren Vollzug der Präsidentin oder dem Präsidenten des Landtags zugewiesen ist, handelt. Im Übrigen gibt sich der Landtag eine seiner verfassungsrechtlichen Stellung entsprechende Daten-

schutzordnung. Sie findet auf die für die Fraktionen und Abgeordneten tätigen Personen entsprechende Anwendung.

(2) Die Landesregierung darf personenbezogene Daten, die für andere Zwecke erhoben worden sind, zur Beantwortung parlamentarischer Anfragen sowie zur Vorlage von Unterlagen und Berichten im Rahmen der Geschäftsordnung des Landtags in dem dafür erforderlichen Umfang verwenden. Dies gilt nicht, wenn die Übermittlung der Daten wegen ihres streng persönlichen Charakters für die Betroffenen unzumutbar ist. Besondere gesetzliche Übermittlungsverbote bleiben unberührt.

(3) Von der Landesregierung übermittelte personenbezogene Daten dürfen nicht in Landtagsdrucksachen aufgenommen oder in sonstiger Weise allgemein zugänglich gemacht werden. Dies gilt nicht, wenn keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange der Betroffenen beeinträchtigt werden.

(4) Abs. 2 gilt entsprechend für die Verwaltungsbehörden der Gemeinden und Landkreise im Rahmen ihrer jeweiligen Auskunftspflichten nach der Hessischen Gemeindeordnung und der Hessischen Landkreisordnung.

Zweiter Abschnitt Rechte der betroffenen Person

§ 31

Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

(1) Die Pflicht zur Information der betroffenen Person nach Art. 13 Abs. 3 der Verordnung (EU) Nr. 2016/679 besteht ergänzend zu der in Art. 13 Abs. 4 der Verordnung (EU) Nr. 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung

1. eine Weiterverarbeitung analog gespeicherter Daten betrifft, bei der sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet, der Zweck mit dem Erhebungszweck nach der Verordnung (EU) Nr. 2016/679 vereinbar ist, die Kommunikation mit der betroffenen Person nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere mit Blick auf den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist,
2.
 - a) die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Art. 23 Abs. 1 Buchst. a bis e der Verordnung (EU) Nr. 2016/679 gefährden,
 - b) die öffentliche Sicherheit oder Ordnung gefährden,
 - c) die Rechte oder Freiheiten Dritter gefährden,
 - d) die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen oder
 - e) sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten

würde und das Interesse des Verantwortlichen an der Nichterteilung der Information das Informationsinteresse der betroffenen Person überwiegt.

Die Entscheidung trifft die Leitung der öffentlichen Stelle oder eine von ihr bestimmte, bei der öffentlichen Stelle beschäftigte Person.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Abs. 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Art. 13 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat. Satz 1 und 2 finden in den Fällen des Abs. 1 Satz 1 Nr. 2 Buchst. d und Nr. 3 keine Anwendung.

(3) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Abs. 1 wegen eines vorübergehenden Hinderungsgrundes, kommt der Verantwortliche der Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Fortfall des Hinderungsgrundes, spätestens jedoch innerhalb von zwei Wochen, nach.

§ 32

Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden

(1) Die Pflicht zur Information der betroffenen Person nach Art. 14 Abs. 1, 2 und 4 der Verordnung (EU) Nr. 2016/679 besteht ergänzend zu den in Art. 14 Abs. 5 der Verordnung (EU) Nr. 2016/679 und § 26 Abs. 1 genannten Ausnahmen nicht, wenn die Erteilung der Information

1. die ordnungsgemäße Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Art. 23 Abs. 1 Buchst. a bis e der Verordnung (EU) Nr. 2016/679 gefährden,
2. die öffentliche Sicherheit oder Ordnung gefährden,
3. die Rechte oder Freiheiten Dritter gefährden oder
4. sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten

würde und das Interesse des Verantwortlichen an der Nichterteilung der Information das Informationsinteresse der betroffenen Person überwiegt. Die Entscheidung trifft die Leitung der öffentlichen Stelle oder eine von ihr bestimmte, bei der öffentlichen Stelle beschäftigte Person.

(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Abs. 1, ergreift der Verantwortliche geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Art. 14 Abs. 1 und 2 der Verordnung (EU) Nr. 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat.

(3) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten durch öffentliche Stellen an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Ab-

schirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

§ 33

Auskunftsrecht der betroffenen Person

(1) Das Recht auf Auskunft der betroffenen Person nach Art. 15 der Verordnung (EU) Nr. 2016/679 besteht ergänzend zu den in § 24 Abs. 2, § 25 Abs. 2 und § 26 Abs. 2 genannten Ausnahmen nicht, wenn

1. die betroffene Person nach § 32 Abs. 1 oder 3 nicht zu informieren ist, oder
2. die Daten
 - a) nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder
 - b) ausschließlich Zwecken der Datensicherung, der Datenschutzkontrolle oder der Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dienen.

(2) Die Gründe der Auskunftsverweigerung sind zu dokumentieren. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Maßgabe des Art. 18 der Verordnung (EU) Nr. 2016/679 einzuschränken.

(3) Wird der betroffenen Person keine Auskunft erteilt, kann sie ihr Auskunftsrecht auch über die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie nach Art. 77 der Verordnung (EU) Nr. 2016/679 die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten anrufen oder gerichtlichen Rechtsschutz suchen kann. Die oder der Hessische Datenschutzbeauftragte hat die betroffene Person darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie oder ihn stattgefunden hat. Die Mitteilung der oder des Hessischen Datenschutzbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Die oder der Hessische Datenschutzbeauftragte hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

(4) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Statt einer Auskunft über personenbezogene Daten kann der betroffenen Person Akteneinsicht gewährt werden.

§ 34

Recht auf Löschung („Recht auf Vergessenwerden“)

(1) Ist eine Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten nach Art. 17 Abs. 1 der Verordnung (EU) Nr. 2016/679 ergänzend zu den in Art. 17 Abs. 3 der Verordnung (EU) Nr. 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung nach Art. 18 der Verordnung (EU) Nr. 2016/679. Satz 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden. Satz 1 bis 3 gelten bis zum 31. Dezember 2024 auch bei automatisierter Datenverarbeitung.

(2) Ergänzend zu Art. 18 Abs. 1 Buchst. b und c der Verordnung (EU) Nr. 2016/679 gilt Abs. 1 Satz 1 und 2 entsprechend im Fall des Art. 17 Abs. 1 Buchst. a und d der Verordnung (EU) Nr. 2016/679, solange und soweit der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Der Verantwortliche unterrichtet die betroffene Person über die Einschränkung der Verarbeitung, sofern sich die Unterrichtung nicht als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde.

(3) Ergänzend zu Art. 17 Abs. 3 Buchst. b der Verordnung (EU) Nr. 2016/679 gilt Abs. 1 entsprechend im Fall des Art. 17 Abs. 1 Buchst. a der Verordnung (EU) Nr. 2016/679, wenn einer Löschung satzungsmäßige Aufbewahrungsfristen entgegenstehen.

§ 35

Widerspruchsrecht

Das Recht auf Widerspruch nach Art. 21 Abs. 1 der Verordnung (EU) Nr. 2016/679 besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

Dritter Abschnitt

Sanktionen

§ 36

Anwendung der Vorschriften über das Bußgeld- und Strafverfahren bei Verstößen nach Artikel 83 der Verordnung (EU) Nr. 2016/679

(1) Für Verstöße nach Art. 83 Abs. 4 bis 6 der Verordnung (EU) Nr. 2016/679 gilt, soweit dieses Gesetz nichts anderes bestimmt, § 41 Abs. 1 Satz 1 und 2 sowie Abs. 2 des Bundesdatenschutzgesetzes entsprechend.

(2) Wegen eines Verstoßes gegen Art. 83 Abs. 4 bis 6 der Verordnung (EU) Nr. 2016/679 werden gegen Behörden und sonstige öffentliche Stellen nach § 2 Abs. 1 Satz 1 keine Geldbußen verhängt.

(3) Eine Meldung nach Art. 33 der Verordnung (EU) Nr. 2016/679 oder eine Benachrichtigung nach Art. 34 Abs. 1 der Verordnung (EU) Nr. 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen die meldepflichtige oder benachrichtigende Person oder ihre in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung der meldepflichtigen oder benachrichtigenden Person verwendet werden.

§ 37

Strafvorschriften

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht,

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(2) Abs. 1 findet nur Anwendung, soweit die Tat nicht in anderen Vorschriften mit einer schwereren Strafe bedroht ist.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche und die oder der Hessische Datenschutzbeauftragte.

(4) Eine Meldung nach Art. 33 der Verordnung (EU) Nr. 2016/679 oder eine Benachrichtigung nach Art. 34 Abs. 1 der Verordnung (EU) Nr. 2016/679 darf in einem Strafverfahren gegen die meldepflichtige oder benachrichtigende Person oder ihre in § 52 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung der meldepflichtigen oder benachrichtigenden Person verwendet werden.

§ 38

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 22 Abs. 2 Satz 2 personenbezogene Daten für andere Zwecke verarbeitet, als für die sie übermittelt wurden.

(2) Die Ordnungswidrigkeit nach Abs. 1 kann mit einer Geldbuße von bis zu fünfzigtausend Euro geahndet werden.

Vierter Abschnitt

Gemeinsame Verfahren, Gemeinsam Verantwortliche

§ 39

Gemeinsame Verfahren, Gemeinsam Verantwortliche

(1) Die Einrichtung eines Verfahrens, das mehreren Verantwortlichen als gemeinsam Verantwortliche im Sinne von Art. 26 der Verordnung (EU) Nr. 2016/679 die Verarbeitung personenbezogener Daten ermöglicht, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist.

(2) Über die in Art. 26 der Verordnung (EU) Nr. 2016/679 genannten Festlegungen hinaus bestimmen die gemeinsam Verantwortlichen eine Stelle, der die Planung, Einrichtung und Durchführung des gemeinsamen Verfahrens obliegt.

(3) Abs. 1 und 2 gelten entsprechend, wenn innerhalb einer öffentlichen Stelle ein gemeinsames Verfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird.

DRITTER TEIL

Bestimmungen für Verarbeitungen zu Zwecken nach Artikel 1 Absatz 1 der Richtlinie (EU) Nr. 2016/680

Erster Abschnitt
Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze
für die Verarbeitung personenbezogener Daten

§ 40
Anwendungsbereich

(1) Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständigen öffentlichen Stellen. Dies gilt, soweit die öffentlichen Stellen zum Zwecke der Erfüllung dieser Aufgaben personenbezogene Daten verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche.

(2) Abs. 1 findet auch Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung und den Vollzug von Strafen, von Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs, von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes und von Geldbußen zuständig sind.

(3) Soweit dieser Teil Vorschriften für Auftragsverarbeiter enthält, gilt er auch für diese.

§ 41
Begriffsbestimmungen

Im Sinne des Dritten Teils

1. sind 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. ist Verarbeitung jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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. ist Einschränkung der Verarbeitung die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;
4. ist Profiling jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. ist Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen 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 personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;
6. ist 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. ist zuständige Behörde
 - a) eine staatliche Stelle, die für die Aufgaben nach § 40 zuständig ist, oder
 - b) eine andere staatliche Stelle oder Einrichtung, der durch Rechtsvorschrift die Ausübung öffentlicher Gewalt und hoheitlicher Befugnisse zur Erfüllung der Aufgaben nach § 40 übertragen wurde;
8. ist Verantwortlicher die zuständige Behörde, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;
9. ist Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;
10. ist 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 Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften nach den Zwecken der Verarbeitung;
11. ist Verletzung des Schutzes personenbezogener Daten eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;
12. sind genetische Daten personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern und insbesondere aus der Analyse einer biologischen Probe der Person gewonnen wurden;
13. sind biometrische Daten mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürli-

- chen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;
14. sind 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. sind 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. ist Aufsichtsbehörde eine von einem Mitgliedstaat nach Art. 41 der Richtlinie (EU) Nr. 2016/680 eingerichtete unabhängige staatliche Stelle;
 17. ist internationale Organisation eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine von zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde;
 18. ist 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 personenbezogenen Daten einverstanden ist.

§ 42

Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Personenbezogene Daten müssen

1. auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,
2. für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,
3. dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung nicht außer Verhältnis zu diesem Zweck stehen,

4. 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. nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, und
6. 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.

Zweiter Abschnitt **Rechtsgrundlagen für die Verarbeitung personenbezogener Daten**

§ 43

Verarbeitung besonderer Kategorien personenbezogener Daten

- (1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.
- (2) Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorzusehen. Geeignete Garantien 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 der verantwortlichen Stelle,
 5. die von anderen Daten getrennte Verarbeitung,
 6. die Pseudonymisierung personenbezogener Daten,
 7. die Verschlüsselung personenbezogener Daten oder
 8. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen.

§ 44

Verarbeitung zu anderen Zwecken

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 der in § 40 genannten

Zwecke handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten und die Verarbeitung zu diesem Zweck erforderlich und verhältnismäßig ist. Die Verarbeitung personenbezogener Daten zu einem anderen, in § 40 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

§ 45

Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken, archivaren oder statistischen Zwecken

(1) Personenbezogene Daten dürfen im Rahmen der in § 40 genannten Zwecke zu wissenschaftlichen oder historischen Forschungszwecken, archivaren oder statistischen Zwecken verarbeitet werden, wenn

1. die betroffene Person nach § 46 eingewilligt hat oder
2. hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorgesehen werden.

Geeignete Garantien nach Satz 1 Nr. 2 können in einer so zeitnah wie möglich erfolgenden 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.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Fall des Abs. 1 Satz 1 Nr. 2 muss darüber hinaus zu wissenschaftlichen oder historischen Forschungszwecken, archivaren oder statistischen Zwecken unbedingt erforderlich sein und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung überwiegen.

(3) Der Verantwortliche sieht im Fall des Abs. 2 angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Personen nach § 43 Abs. 2 vor. Ergänzend zu den in § 43 Abs. 2 genannten Maßnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechnete Interessen der betroffenen Person stehen dem entgegen. Sobald der Forschungs- oder Statistikzweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern; die Merkmale sind zu löschen, sobald der Forschungs- oder Statistikzweck dies zulässt. Vor dem Beginn des Forschungsvorhabens ist ein Datenschutzkonzept zu erstellen, das der zuständigen Aufsichtsbehörde auf Nachfrage vorzulegen ist.

(4) Die in den §§ 50 bis 53 vorgesehenen Rechte sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Auskunft besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(5) Das Recht auf Auskunft nach § 52 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen. Das Recht auf Berichtigung der betroffenen Person nach § 53 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öf-

fentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen. Das Recht auf Einschränkung der Verarbeitung nach § 53 besteht nicht, soweit dieses Recht voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich macht oder ernsthaft beeinträchtigt und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

(6) Der Verantwortliche darf personenbezogene Daten zu wissenschaftlichen oder historischen Forschungszwecken nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 46

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 den 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 hiervon in Kenntnis zu setzen. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(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 Einzelfalles 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.

§ 47

Verarbeitung auf Weisung des Verantwortlichen

Der Auftragsverarbeiter und jede einem Verantwortlichen oder dem 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 sind.

§ 48

Datengeheimnis

Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort. Die Personen sind über die bei ihrer Tätigkeit zu beachtenden Vorschriften über den Datenschutz zu unterrichten.

§ 49

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.

(2) Entscheidungen nach Abs. 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

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

Dritter Abschnitt

Rechte der betroffenen Person

§ 50

Allgemeine Informationen zu Datenverarbeitungen

Der Verantwortliche hat in allgemeiner, verständlicher und leicht zugänglicher Form Informationen in einer klaren und einfachen Sprache zur Verfügung zu stellen über

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 die Kontaktdaten der oder des Datenschutzbeauftragten,
4. das Recht, die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten anzurufen, und
5. die Erreichbarkeit der oder des Hessischen Datenschutzbeauftragten.

§ 51

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 § 50 genannten Angaben,
2. die Rechtsgrundlage der Verarbeitung,
3. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten, auch der Empfänger in Drittländern oder in internationalen Organisationen, sowie
5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

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

1. die
 - a) Erfüllung der in § 40 genannten Aufgaben,
 - b) öffentliche Sicherheit oder
 - c) Rechte oder Freiheiten Dritter

gefährdet würden oder

2. dem Wohle des Bundes oder eines Landes Nachteile bereitet würden

und wenn das Interesse des Verantwortlichen an der Nichterteilung der Information das Informationsinteresse der betroffenen Person überwiegt. Die Entscheidung trifft die Leitung der öffentlichen Stelle oder eine von ihr bestimmte, bei der öffentlichen Stelle beschäftigte Person.

(3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Im Fall der Einschränkung nach Abs. 2 gilt § 52 Abs. 7 entsprechend.

§ 52 **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 Drittländern 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 § 55, die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten anzurufen, sowie
8. Angaben zur Erreichbarkeit der oder des Hessischen Datenschutzbeauftragten.

(2) Abs. 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, der Datenschutzkontrolle oder der Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage dienen.

(3) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht. Statt einer Auskunft über personenbezogene Daten kann der betroffenen Person Akteneinsicht gewährt werden.

(4) Der Verantwortliche kann unter den Voraussetzungen des § 51 Abs. 2 von der Auskunft nach Abs. 1 Satz 1 absehen oder die Auskunftserteilung nach Abs. 1 Satz 2 teilweise oder vollständig einschränken.

(5) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(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 § 51 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 Abs. 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie nach § 55 die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten anrufen oder gerichtlichen Rechtsschutz suchen kann. Die oder der Hessische Datenschutzbeauftragte hat die betroffene Person darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie oder ihn stattgefunden hat. Die Mitteilung der oder des Hessischen Datenschutzbeauftragten an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Die oder der Hessische Datenschutzbeauftragte 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.

§ 53

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 Bewertungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Bewertung. 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 die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke 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 Beweis Zwecken weiter aufbewahrt werden müssen oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck, der ihrer Löschung entgegenstand, oder sonst mit Einwilligung der betroffenen Person verarbeitet werden.

(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 der Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach Abs. 1 bis 3 hat der Verantwortliche Empfängern, denen die Daten übermittelt wurden, diese Maßnahmen mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken.

(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, soweit bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 51 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) § 52 Abs. 7 und 8 findet entsprechende Anwendung.

§ 54

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. Unbeschadet besonderer Formvorschriften soll er bei der Beantwortung von Anträgen die für den Antrag gewählte Form verwenden. Bei der Auswahl des Mediums sind die Anforderungen des § 59 zu beachten.

(2) Bei Anträgen hat der Verantwortliche die betroffene Person unbeschadet des § 52 Abs. 6 und des § 53 Abs. 6 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie mit diesen Anträgen verfahren wurde.

(3) Die Erteilung von Informationen nach § 50, die Benachrichtigungen nach den §§ 51 und 61 und die Bearbeitung von Anträgen nach den §§ 52 und 53 erfolgen verwaltungskostenfrei. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den §§ 52 und 53 kann der Verantwortliche entweder eine angemessene Gebühr auf der Grundlage des Verwaltungsaufwands 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 den §§ 52 und 53 gestellt hat, kann er von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 55

Anrufung der oder des Hessischen Datenschutzbeauftragten

(1) Jede betroffene Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen zu den in § 40 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 Hessische Datenschutzbeauftragte hat die betroffene Person über den Stand und das Ergebnis der Beschwerde zu unterrichten und sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes nach § 56 hinzuweisen.

(2) Die oder der Hessische Datenschutzbeauftragte hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer anderen Aufsichtsbehörde fällt, unverzüglich an diese 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.

§ 56

Rechtsschutz gegen Entscheidungen der oder des Hessischen Datenschutzbeauftragten oder bei deren oder dessen Untätigkeit

(1) Jede natürliche oder juristische Person kann unbeschadet anderer Rechtsbehelfe gerichtlich gegen eine sie betreffende verbindliche Entscheidung der oder des Hessischen Datenschutzbeauftragten vorgehen.

(2) Abs. 1 gilt entsprechend zugunsten betroffener Personen, wenn sich die oder der Hessische Datenschutzbeauftragte mit einer Beschwerde nach § 55 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.

Vierter Abschnitt Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 57

Auftragsverarbeitung

(1) Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften 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 keine 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 Abs. 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 nach § 71 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;
6. Überprüfungen, die von dem Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt;
7. die in den Abs. 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;
8. alle nach § 59 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 §§ 59 bis 62 und 64 genannten Pflichten unterstützt.

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

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

§ 58

Gemeinsame Verfahren, Gemeinsam Verantwortliche

(1) Die Einrichtung eines Verfahrens, das mehreren Verantwortlichen als gemeinsam Verantwortliche die Verarbeitung personenbezogener Daten ermöglicht, ist nur zulässig, wenn dies unter Berücksichtigung der schutzwürdigen Belange der betroffenen Personen und der Aufgaben der beteiligten Stellen angemessen ist.

(2) Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als gemeinsam Verantwortliche.

(3) Gemeinsam Verantwortliche haben eine Stelle zu bestimmen, der die Planung, Einrichtung und Durchführung des gemeinsamen Verfahrens obliegt, und ihre jeweiligen Aufgaben sowie 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 be-

troffene Person nicht, ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen.

(4) Abs. 1 bis 3 gelten entsprechend, wenn innerhalb einer öffentlichen Stelle ein gemeinsames Verfahren zur Verarbeitung personenbezogener Daten für verschiedene Zwecke eingerichtet wird.

§ 59

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 des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische 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. Eintrittswahrscheinlichkeit und Schwere der Verletzung sollen nach der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung bestimmt und anhand einer objektiven Beurteilung der Höhe des Risikos festgestellt werden.

(2) Die in Abs. 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 Abs. 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 mithilfe 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 welche Stellen personenbezogene Daten mithilfe 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 Störfall 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.

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

§ 60

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten

(1) Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem sie ihm bekannt geworden ist, der oder dem Hessischen Datenschutzbeauftragten zu melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Erfolgt die Meldung an die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. § 59 Abs. 1 Satz 2 gilt entsprechend.

(2) Wird dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt, meldet er diese dem Verantwortlichen unverzüglich.

(3) Die Meldung nach Abs. 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 Personen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat,
2. den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten und
4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behandlung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls der Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

(4) Wenn und soweit die Informationen nach Abs. 3 nicht zur gleichen Zeit bereitgestellt werden können, hat der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.

(5) Der Verantwortliche hat 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 Abs. 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

(7) § 37 Abs. 4 findet entsprechende Anwendung.

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

§ 61

Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten

(1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich von der Verletzung zu benachrichtigen. § 59 Abs. 1 Satz 2 gilt entsprechend.

(2) Die Benachrichtigung nach Abs. 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in § 60 Abs. 3 Nr. 2 bis 4 genannten Informationen und Maßnahmen zu enthalten.

(3) Die Benachrichtigung der betroffenen Person nach Abs. 1 ist nicht erforderlich, wenn

1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht werden;
2. der Verantwortliche durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen im Sinne des Abs. 1 nicht 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 Hessische Datenschutzbeauftragte verlangen, dies nachzuholen, oder verbindlich feststellen, dass bestimmte der in Abs. 3 genannten Voraussetzungen erfüllt sind. Hierbei hat sie oder er die Wahrscheinlichkeit zu berücksichtigen, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko im Sinne des Abs. 1 führt.

(5) Die Benachrichtigung der betroffenen Personen nach Abs. 1 kann unter den in § 51 Abs. 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund des von der Verletzung ausgehenden hohen Risikos im Sinne des Abs. 1 überwiegen.

(6) § 37 Abs. 4 findet entsprechende Anwendung.

§ 62

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 Rechte und Freiheiten natürlicher Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. § 59 Abs. 1 Satz 2 gilt entsprechend.

(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 Folgenabschätzung zu beteiligen.

(4) Die Folgenabschätzung hat den Rechten und den berechtigten Interessen der von der Verarbeitung betroffenen Personen und sonstiger Betroffener Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung,
2. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck,
3. eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und
4. die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, 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 Folgenabschätzung ergeben haben.

§ 63

Zusammenarbeit mit der oder dem Hessischen Datenschutzbeauftragten

Der Verantwortliche und der Auftragsverarbeiter haben mit der oder dem Hessischen Datenschutzbeauftragten bei der Erfüllung ihrer oder seiner Aufgaben zusammenzuarbeiten.

§ 64

Vorherige Konsultation der oder des Hessischen Datenschutzbeauftragten

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten zu konsultieren, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 62 hervorgeht, dass die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, oder
2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge hat.

Die oder der Hessische Datenschutzbeauftragte kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur vorherigen Konsultation nach Satz 1 unterliegen. § 59 Abs. 1 Satz 2 gilt entsprechend.

(2) Der oder dem Hessischen Datenschutzbeauftragten sind im Fall des Abs. 1 vorzulegen:

1. die nach § 62 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 Rechte und Freiheiten der betroffenen Personen vorgesehenen Maßnahmen und Garantien und
5. die Kontaktdaten der oder des Datenschutzbeauftragten.

Auf Anfrage sind der oder dem Hessischen Datenschutzbeauftragten 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 Personen bestehenden Risiken und die diesbezüglichen Garantien bewerten zu können.

(3) Falls die oder der Hessische Datenschutzbeauftragte der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, kann sie oder er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu sechs Wochen nach Erhalt des Ersuchens um Konsultation schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Die oder der Hessische Datenschutzbeauftragte 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 Eingang des Antrags auf Konsultation den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zusammen mit den Gründen für die Verzögerung zu informieren.

(4) 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 vorherigen Konsultation, aber vor Ablauf der in Abs. 3 genannten Frist beginnen. In diesem Fall sind die Empfehlungen der oder des Hessischen Datenschutzbeauftragten im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

(5) Die oder der Hessische Datenschutzbeauftragte ist bei der Ausarbeitung eines Vorschlags für eine vom Landtag zu erlassende Gesetzgebungsmaßnahme oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung personenbezogener Daten betreffen, zu konsultieren.

§ 65

Verzeichnis von Verarbeitungstätigkeiten

(1) Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die seiner Zuständigkeit unterliegen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie 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 sollen, einschließlich Empfängern in Drittländern oder internationalen Organisationen,
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 ein Drittland 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 oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und
9. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 59.

(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 die Kontaktdaten der oder des Datenschutzbeauftragten,
2. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,
3. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, wenn vom Verantwortlichen entsprechend angewiesen, unter Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation und
4. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 59.

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

(4) Verantwortliche und Auftragsverarbeiter haben auf Anfrage ihre Verzeichnisse der oder dem Hessischen Datenschutzbeauftragten zur Verfügung zu stellen.

§ 66

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 technische und organisatorische Maßnahmen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und notwendige Garantien in die Verarbeitung aufzunehmen, um den gesetzlichen Anforderungen zu genügen und die Rechte der betroffenen Personen zu schützen. 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 Risiken für die Rechte und Freiheiten natürlicher 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, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Maßnahmen müssen insbesondere sicherstellen, dass die personenbezogenen Daten durch Voreinstellungen nicht ohne Eingreifen einer Person einer unbestimmten Anzahl von natürlichen Personen zugänglich gemacht werden.

§ 67

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 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 Zeuginnen und Zeugen, Hinweisgeberinnen und Hinweisgeber oder Personen, die mit den in den Nr. 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

§ 68

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 und angemessen ist, Bewertungen, 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 Bewertung zugrunde liegen.

§ 69

Qualitätssicherung personenbezogener Daten vor deren Übermittlung

(1) Der Verantwortliche hat angemessene Maßnahmen zu ergreifen, um zu gewährleisten, dass unrichtige sowie ohne sachlichen Grund unvollständige oder nicht mehr aktuelle personenbezogene Daten nicht übermittelt oder sonst bereitgestellt werden. Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der personenbezogenen Daten vor ihrer Übermittlung

oder Bereitstellung zu überprüfen. Bei jeder Übermittlung personenbezogener Daten hat er, 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 darauf hinzuweisen, dass diese Bedingungen gelten und einzuhalten sind. 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 oder 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.

§ 70

Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung

(1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. § 53 Abs. 1 Satz 2 und 3 ist entsprechend anzuwenden.

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

(3) § 53 Abs. 3 bis 5 ist entsprechend anzuwenden. Sind unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmäßig übermittelt worden, ist auch dies 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.

§ 71

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 und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen.

(3) Die Protokolle dürfen ausschließlich zur Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch die Datenschutzbeauftragte oder den Datenschutzbeauftragten und die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten sowie zur Eigenüberwachung, der Sicherstellung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.

(4) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der oder dem Hessischen Datenschutzbeauftragten auf Anforderung zur Verfügung zu stellen.

§ 72

Vertrauliche Meldung von Verstößen

Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können.

Fünfter Abschnitt

Datenübermittlungen an Drittländer und an internationale Organisationen

§ 73

Allgemeine Voraussetzungen

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

1. die Stelle oder internationale Organisation für die in § 40 genannten Zwecke zuständig ist und
2. die Europäische Kommission nach Art. 36 Abs. 3 der Richtlinie (EU) Nr. 2016/680 einen Angemessenheitsbeschluss gefasst hat.

(2) Die Übermittlung personenbezogener Daten hat trotz des Vorliegens eines Angemessenheitsbeschlusses im Sinne des Abs. 1 Nr. 2 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 Abs. 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 Mitgliedstaats oder eines Drittlandes oder für die wesentlichen Interessen eines Mitgliedstaats abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Im Fall des Satz 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 Abs. 1 übermittelt, hat durch geeignete Maßnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an Stellen in anderen Drittländern 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 Drittland oder der internationalen Organisation, an das 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 die Stelle im anderen Drittland oder die andere internationale Organisation zulässig wäre. Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

§ 74

Datenübermittlung bei geeigneten Garantien

(1) Liegt entgegen § 73 Abs. 1 Nr. 2 kein Beschluss nach Art. 36 Abs. 3 der Richtlinie (EU) Nr. 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 73 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 Abs. 1 Nr. 2 zu dokumentieren. Die Dokumentation hat den Zeitpunkt der Übermittlung, Informationen über die empfangende zuständige Behörde, die Begründung der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. Sie ist der oder dem Hessischen Datenschutzbeauftragten auf Anforderung zur Verfügung zu stellen.

(3) Der Verantwortliche hat die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten zumindest jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Abs. 1 Nr. 2 erfolgt sind. In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

§ 75

Ausnahmen für eine Datenübermittlung ohne geeignete Garantien

(1) Liegt entgegen § 73 Abs. 1 Nr. 2 kein Beschluss nach Art. 36 Abs. 3 der Richtlinie (EU) Nr. 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des § 74 Abs. 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 73 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person,
2. zur Wahrung berechtigter Interessen der betroffenen Person,

3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates,
4. im Einzelfall für die in § 40 genannten Zwecke oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 40 genannten Zwecken.

(2) Der Verantwortliche hat von einer Übermittlung nach Abs. 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

(3) Für Übermittlungen nach Abs. 1 gilt § 74 Abs. 2 und 3 entsprechend.

§ 76

Sonstige Datenübermittlung an Empfänger in Drittländern

(1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittländer geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten unmittelbar an nicht in § 73 Abs. 1 Nr. 1 genannte Stellen in Drittländern übermitteln, wenn die Übermittlung zur Erfüllung ihrer Aufgaben für die in § 40 genannten Zwecke 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 § 73 Abs. 1 Nr. 1 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 Abs. 1 hat der Verantwortliche die in § 73 Abs. 1 Nr. 1 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

(3) Für Übermittlungen nach Abs. 1 gilt § 74 Abs. 2 und 3 entsprechend.

(4) Bei Übermittlungen nach Abs. 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.

Sechster Abschnitt

Zusammenarbeit der Aufsichtsbehörden

§ 77

Gegenseitige Amtshilfe

(1) Die oder der Hessische Datenschutzbeauftragte 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) Nr. 2016/680 erforderlich ist. Die Amtshilfe betrifft insbesondere Auskunftersuchen und aufsichtsbezogene Maßnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

(2) Die oder der Hessische Datenschutzbeauftragte hat alle geeigneten Maßnahmen zu ergreifen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingang nachzukommen.

(3) Die oder der Hessische Datenschutzbeauftragte 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 Hessische Datenschutzbeauftragte 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 Fall des Abs. 3 die Gründe für die Ablehnung des Ersuchens zu erläutern.

(5) Die oder der Hessische Datenschutzbeauftragte hat die Informationen, um die sie oder er von der Aufsichtsbehörde des anderen Staates ersucht wurde, in der Regel elektronisch und in einem standardisierten Format zu übermitteln.

(6) Die oder der Hessische Datenschutzbeauftragte 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 Hessischen Datenschutzbeauftragten 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.

Siebter Abschnitt Haftung und Sanktionen

§ 78

Schadensersatz und Entschädigung

(1) Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder nach 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, welche von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche beziehungsweise sein Rechtsträger.

(4) Bei einem Mitverschulden der betroffenen Person ist § 254 des Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

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

(6) Weitergehende sonstige Schadensersatzansprüche bleiben unberührt.

(7) Der Rechtsweg zu den ordentlichen Gerichten steht offen.

§ 79

Strafvorschriften

Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten nach § 40 findet § 37 entsprechende Anwendung.

VIERTER TEIL

Informationsfreiheit

§ 80

Anspruch auf Informationszugang

(1) Jeder hat nach Maßgabe des Vierten Teils gegenüber öffentlichen Stellen Anspruch auf Zugang zu amtlichen Informationen (Informationszugang). Abweichend von § 2 Abs. 2 Satz 1 gelten insoweit auch öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen, als öffentliche Stellen. Amtliche Informationen sind alle amtlichen Zwecken dienende Aufzeichnungen, unabhängig von der Art ihrer Speicherung. Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen, gehören nicht dazu.

(2) Soweit besondere Rechtsvorschriften die Auskunftserteilung regeln, gehen sie den Vorschriften des Vierten Teils vor.

§ 81

Anwendungsbereich

(1) Nach Maßgabe des § 2 Abs. 1 bis 3 gelten die Vorschriften über den Informationszugang auch für

1. den Landtag, nur soweit er öffentlich-rechtliche Verwaltungsaufgaben wahrnimmt und auszuschließen ist, dass durch die Gewährung des Informationszugangs die Freiheit des Mandats, der Bereich der Abgeordneten- und Fraktionsangelegenheiten sowie die Nichtöffentlichkeit von Landtagsberatungen beeinträchtigt wird,
2. den Hessischen Rechnungshof, die Überörtliche Prüfung kommunaler Körperschaften in Hessen, den Landesbeauftragten für Wirtschaftlichkeit in der Verwaltung, soweit sie Verwaltungsaufgaben wahrnehmen, die nicht in Zusammenhang mit ihrer Kontroll- und Prüftätigkeit stehen,
3. die Hessische Datenschutzbeauftragte oder den Hessischen Datenschutzbeauftragten, soweit sie oder er allgemeine Verwaltungsaufgaben wahrnimmt,

4. die Gerichte, Strafverfolgungs- und Strafvollstreckungsbehörden und sonstige in § 40 Abs. 2 genannten Stellen, jedoch nur soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen und nicht, soweit sie im Rahmen ihrer justiziellen Tätigkeit handeln,
5. Finanzbehörden, nur soweit sie nicht in Verfahren nach der Abgabenordnung tätig werden,
6. Universitätskliniken, Forschungseinrichtungen, Hochschulen, Schulen sowie sonstige öffentliche Stellen, soweit sie nicht in den Bereichen Forschung und Lehre, Leistungsbeurteilungen und Prüfungen tätig werden,
7. die Behörden und sonstigen öffentlichen Stellen der Gemeinden und Landkreise sowie deren Vereinigungen ungeachtet ihrer Rechtsform, soweit die Anwendung des Vierten Teils durch Satzung ausdrücklich bestimmt wird,
8. den Hessischen Rundfunk, soweit er Aufgaben der öffentlichen Verwaltung wahrnimmt, sowie die Hessische Landesanstalt für privaten Rundfunk und neue Medien, soweit sie nicht in den Bereichen Zulassung und Aufsicht tätig wird.

(2) Die Vorschriften des Vierten Teils gelten nicht für

1. die Polizeibehörden und das Landesamt für Verfassungsschutz,
2. die Landeskartellbehörde und die Regulierungskammer Hessen,
3. die Industrie- und Handelskammern und die Handwerkskammern,
4. Notarinnen und Notare,
5. die Disziplinarorgane im Rahmen ihrer disziplinarrechtlichen Tätigkeit.

(3) Soweit ein Informationszugang nach Abs. 1 oder 2 ausgeschlossen ist, gilt dies auch für Datei- und Aktenbestandteile, die sich in Dateien oder Akten anderer öffentlicher Stellen befinden.

§ 82

Schutz besonderer öffentlicher und privater Belange

Ein Anspruch auf Informationszugang besteht nicht

1. bei Verschlusssachen nach § 2 Abs. 1 des Hessischen Sicherheitsüberprüfungsgesetzes vom 19. Dezember 2014 (GVBl. S. 364),
2. bei Informationen, deren Bekanntwerden nachteilige Auswirkungen haben kann auf
 - a) die inter- und supranationalen Beziehungen, die Beziehung zum Bund oder zu einem anderen Land,
 - b) Belange der äußeren oder öffentlichen Sicherheit,

- c) die Kontroll-, Vollzugs- oder Aufsichtsaufgaben der Finanz-, Regulierungs-, Sparkassen, Versicherungs- und Wettbewerbsaufsichtsbehörden oder
 - d) den Erfolg eines strafrechtlichen Ermittlungs- oder Strafvollstreckungsverfahrens oder den Verfahrensablauf eines Gerichts-, Ordnungswidrigkeiten- oder Disziplinarverfahrens,
3. bei einem Berufs- oder besonderen Amtsgeheimnis unterliegenden Datei- oder Akteninhalten,
 4. bei zum persönlichen Lebensbereich gehörenden Geheimnissen oder Betriebs- oder Geschäftsgeheimnissen, sofern die betroffene Person nicht eingewilligt hat oder
 5. soweit ein rein wirtschaftliches Interesse an den Informationen besteht.

§ 83

Schutz personenbezogener Daten

Der Informationszugang zu personenbezogenen Daten ist nur dann und soweit zulässig, wie ihre Übermittlung an eine nicht öffentliche Stelle zulässig ist.

§ 84

Schutz behördlicher Entscheidungsprozesse

(1) Der Antrag auf Informationszugang kann abgelehnt werden für Entwürfe zu Entscheidungen sowie für Arbeiten und Beschlüsse zu ihrer unmittelbaren Vorbereitung, soweit und solange durch die vorzeitige Bekanntgabe der Informationen der Erfolg der Entscheidung oder bevorstehender behördlicher Maßnahmen vereitelt würde. Nicht der unmittelbaren Entscheidungsvorbereitung nach Satz 1 dienen regelmäßig Ergebnisse der Beweiserhebung und Gutachten oder Stellungnahmen Dritter.

(2) Der Antrag auf Informationszugang ist abzulehnen,

1. wenn die Bekanntgabe der Information den Kernbereich der Willens- und Entscheidungsbildung der Landesregierung betrifft, oder
2. zu Protokollen vertraulicher Beratungen.

In den Fällen des Satz 1 besteht nach Abschluss des Entscheidungsprozesses Anspruch auf Informationszugang zu den Ergebnisprotokollen, soweit sie nicht vertraulich sind.

§ 85

Antrag

(1) Ein Informationszugang wird auf Antrag bei der Stelle, die über die begehrten Informationen verfügt (informationspflichtige Stelle) gewährt. Ist die angerufene Stelle nicht die informationspflichtige Stelle, soll sie der antragstellenden Person die informationspflichtige Stelle benennen.

(2) Im Antrag sollen die begehrten Informationen möglichst genau umschrieben werden. Ein Antrag, der auf allgemeines Behördenhandeln gerichtet ist und sich auf Informationen bezieht, die aus einer Vielzahl von Aktenvorgängen oder Informationsträgern zusammengetragen werden müssen, kann abgelehnt werden, wenn der Informationszugang nur mit unverhältnismäßigem Verwaltungsaufwand

möglich wäre. Sofern der antragstellenden Person Angaben zur Umschreibung der begehrten Informationen fehlen, ist die angerufene informationspflichtige Stelle zur Beratung verpflichtet.

(3) Betrifft der Antrag Daten Dritter im Sinne der §§ 82 und 83, muss er begründet werden.

§ 86

Verfahren bei Beteiligung Dritter

Die informationspflichtige Stelle gibt einem Dritten, dessen Belange durch den Antrag auf Informationszugang berührt sind, schriftlich Gelegenheit zur Stellungnahme innerhalb eines Monats, sofern Anhaltspunkte dafür vorliegen, dass er ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann. Die Einwilligung des Dritten zum Informationszugang der antragstellenden Person gilt als verweigert, wenn sie nicht innerhalb eines Monats nach Anfrage durch die zuständige Stelle vorliegt.

§ 87

Entscheidung

(1) Die informationspflichtige Stelle hat unverzüglich, spätestens innerhalb eines Monats, in den Fällen des § 86 spätestens innerhalb von drei Monaten nach Eingang des hinreichend bestimmten Antrags zu entscheiden. In den Fällen des § 86 ist die Entscheidung auch dem Dritten bekannt zu geben.

(2) Soweit dem Antrag stattgegeben wird, sind die Informationen innerhalb der in Abs. 1 Satz 1 genannten Frist zugänglich zu machen. In den Fällen des § 86 darf der Informationszugang erst gewährt werden, wenn die Entscheidung dem Dritten gegenüber bestandskräftig ist oder die sofortige Vollstreckung angeordnet wurde und seit der Bekanntgabe der Anordnung an den Dritten zwei Wochen verstrichen sind.

(3) Die Ablehnung oder teilweise Ablehnung des beantragten Informationszugangs ist innerhalb der in Abs. 1 Satz 1 genannten Frist schriftlich bekannt zu geben und zu begründen. Darüber hinaus ist mitzuteilen, ob und wann ein Informationszugang ganz oder teilweise zu einem späteren Zeitpunkt voraussichtlich möglich sein könnte.

(4) Können die Informationen nicht oder nicht vollständig innerhalb der in Abs. 1 Satz 1 genannten Fristen zugänglich gemacht werden oder erfordern Umfang oder Komplexität eine intensive Prüfung, so kann die informationspflichtige Stelle die Frist um einen Monat verlängern. Die antragstellende Person ist über die Fristverlängerung unter Angabe der maßgeblichen Gründe schriftlich zu informieren.

(5) Für Streitigkeiten nach diesem Teil des Gesetzes ist der Verwaltungsrechtsweg gegeben. Ein Vorverfahren nach § 68 der Verwaltungsgerichtsordnung findet nicht statt.

§ 88

Kosten

(1) Die Erteilung mündlicher und einfacher schriftlicher Auskünfte sowie die Einsichtnahme in Dateien und Akten vor Ort nach dem Vierten Teil dieses Gesetzes sind kostenfrei. Für sonstige Amtshandlungen nach diesem Teil werden Kosten (Gebühren und Auslagen) nach Maßgabe des Hessischen Verwaltungskostengesetzes erhoben. Von § 9 des Hessischen Verwaltungskostengesetzes gelten nur Abs. 1 Satz 1 Nr. 6, insoweit mit der Maßgabe, dass Auslagen für Ausfertigungen, Abschriften und Kopien 0,20 Euro je Seite nicht überschreiten dürfen, und Abs. 5. Die Gebühren sind auch unter Berücksichtigung des Verwaltungsaufwandes so zu bemessen, dass die antragstellenden Personen dadurch nicht von der Geltendmachung ihres Informationsanspruchs nach § 80 Abs. 1 abgehalten werden.

(2) Im Fall des § 81 Abs. 1 Nr. 7 werden Kosten nach Maßgabe der Satzung erhoben.

§ 89

Die oder der Hessische Informationsfreiheitsbeauftragte

(1) Jeder, der sich in seinem Recht nach dem Vierten Teil verletzt sieht, kann unbeschadet anderweitiger Rechtsbehelfe die Hessische Informationsfreiheitsbeauftragte oder den Hessischen Informationsfreiheitsbeauftragten anrufen.

(2) Die Aufgabe der oder des Hessischen Informationsfreiheitsbeauftragten wird von der oder dem Hessischen Datenschutzbeauftragten wahrgenommen.

(3) Die auskunftspflichtigen Stellen sind verpflichtet, die Hessische Informationsfreiheitsbeauftragte oder den Hessischen Informationsfreiheitsbeauftragten und ihre oder seine Beauftragten in der Erfüllung ihrer Aufgaben zu unterstützen. Der oder dem Hessischen Informationsfreiheitsbeauftragten ist dabei insbesondere

1. hinsichtlich des Anliegens, dessentwegen sie oder er angerufen wurde, Auskunft zu erteilen und Einsicht in betreffenden Dateien und Akten zu verschaffen und
2. Zutritt zu den Diensträumen zu gewähren.

Stellt die oder der Hessische Informationsfreiheitsbeauftragte Verstöße gegen die Vorschriften des Vierten Teils fest, kann sie oder er ihre Behebung in angemessener Frist fordern. Darüber ist die zuständige Aufsichtsbehörde zu unterrichten.

(4) Zum 31. Dezember jedes Jahres hat die oder der Hessische Informationsfreiheitsbeauftragte dem Landtag und der Landesregierung einen Bericht über ihre oder seine Tätigkeit vorzulegen. Die Landesregierung legt ihre Stellungnahme zu dem Bericht dem Landtag vor.

FÜNFTER TEIL

Übergangs- und Schlussvorschriften

§ 90

Übergangsvorschriften

(1) Vor dem 6. Mai 2016 eingerichtete automatisierte Verarbeitungssysteme sind zeitnah, in Ausnahmefällen, in denen dies mit einem unverhältnismäßigen Aufwand verbunden ist, jedoch spätestens bis zum 6. Mai 2023, mit § 71 Abs. 1 und 2 in Einklang zu bringen.

(2) Für die Person, die am 24. Mai 2018 das Amt der oder des Hessischen Datenschutzbeauftragten innehat, gilt bis zur ersten Wahl der oder des Hessischen Datenschutzbeauftragten nach dem 25. Mai 2018 § 21 Abs. 4 Satz 1 in der bis zum 24. Mai 2018 geltenden Fassung fort.

§ 91

Inkrafttreten

Dieses Gesetz tritt am 25. Mai 2018 in Kraft.

Anlage:

Verwaltungskostenverzeichnis

Nr.	Gegenstand	Bemessungs- grundlage	Gebühr EUR
1	2	3	4
1	Gebühren		
11	Auskünfte, Akteneinsicht		
111	schriftliche Auskünfte Einfache schriftliche Auskünfte sind kostenfrei, soweit sie nicht aus Registern oder Dateien erteilt werden.		30 bis 600
112	Gewährung von Einsicht in amtliche Akten, Karteien, Datenträger usw. Die Auslagen sind mit der Gebühr nach Nr. 1121 bis 1123 abgegolten.		
1121	für Personen, die nicht am Verfahren beteiligt sind oder deren Verfahren abgeschlossen ist und die nicht betroffene Person im Sinne der Verordnung (EU) Nr. 2016/679 sind		10 bis 600
1122	für Personen, die am Verfahren beteiligt sind, aber nicht betroffene Person im Sinne der Verordnung (EU) Nr. 2016/679 sind		kostenfrei
1123	zusätzlich 1121 oder 1122 für das Versenden von Akten oder Kopien aus Akten, auch von Bußgeldakten außerhalb eines Bußgeldverfahrens	je Sendung	12
12	Missbrauchsgebühr		
121	Missbrauchsgebühr nach Art. 57 Abs. 4 der Verordnung (EU) Nr. 2016/679 oder § 13 Abs. 10		100 bis 1 000
13	Überprüfungen der Datenverarbeitungen nach der Verordnung (EU) Nr. 2016/679		

131	Überprüfung der Datenverarbeitung nach Art. 57 Abs. 1 Buchst. a mit besonderem Verwaltungsaufwand Die Gebühr wird nur erhoben, wenn ein Verstoß festgestellt und eine Maßnahme nach Art. 58 Abs. 2 Buchst. b bis g getroffen wird.		500 bis 15 000
132	Aussetzung einer Übermittlung von Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation nach Art. 58 Abs. 2 Buchst. j		500 bis 5 000
14	Stellungnahmen und Genehmigungen nach der Verordnung (EU) Nr. 2016/679		
141	Beratung im Rahmen einer Datenschutz-Folgenabschätzung nach Art. 58 Abs. 3 Buchst. a einschließlich einer Genehmigung nach Art. 36 Abs. 5		500 bis 5 000
142	Stellungnahme zu und Billigung von Verhaltensregeln nach Art. 58 Abs. 3 Buchst. d in Verbindung mit Art. 40 Abs. 5		500 bis 5 000
143	Erteilung einer Zertifizierung oder Billigung von Kriterien für eine Zertifizierung nach Art. 58 Abs. 3 Buchst. f in Verbindung mit Art. 42 Abs. 5		1 000 bis 30 000
144	Genehmigung von Vertragsklauseln nach Art. 58 Abs. 3 Buchst. h in Verbindung mit Art. 46 Abs. 3 Buchst. a		500 bis 15 000
145	Genehmigung von verbindlichen internen Vorschriften nach Art. 58 Abs. 3 Buchst. j in Verbindung mit Art. 47		500 bis 15 000
2	Auslagen		
21	Anfertigung von Kopien unabhängig von der Art der Herstellung bis DIN A 3 - die vom Kostenschuldner besonders beantragt	je Seite	0,20

	oder - die aus vom Kostenschuldner zu vertretenden Gründen notwendig wurden		
--	--	--	--