

G e s e t z e n t w u r f

der Landesregierung

Thüringer Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Thüringer Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - ThürDSAnpUG-EU -)

A. Problem und Regelungsbedürfnis

Am 25. Mai 2018 wird die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) unmittelbar geltendes Recht in allen Mitgliedstaaten der Europäischen Union sein. Ziel der Verordnung ist die Schaffung eines gleichmäßigen und hohen Datenschutzniveaus für natürliche Personen in der Union (Erwägungsgrund 10). Grundsätzlich gelten europarechtliche Verordnungen unmittelbar (Artikel 288 Abs. 2 des Vertrages über die Arbeitsweise der Europäischen Union - AEU-Vertrag -). Sie bedürfen keiner Umsetzung in den Mitgliedstaaten. Es handelt sich bei dem Datenschutzrecht allerdings um eine national stark vorgeprägte Rechtsmaterie, so dass die Mitgliedstaaten im Zuge der Verhandlungen zur Verordnung (EU) 2016/679 zahlreiche Regelungsmöglichkeiten in deren Anwendungsbereich durchgesetzt haben. Dies betrifft vor allem den Datenschutz bei der Datenverarbeitung durch öffentliche Stellen. Daher regelt die Verordnung (EU) 2016/679 den Datenschutz nur im Grundsatz abschließend, was sich bereits in ihrem Titel "Datenschutz-Grundverordnung" abzeichnet. Damit eröffnet sie die Möglichkeit, die Grundsätze und Ziele, welche sich im Rahmen der Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31; L 40 vom 17.2.2017, S. 78) in den Mitgliedstaaten entwickelt haben sowie nationale Besonderheiten und Schutzstandards, in wesentlichen Teilen beizubehalten beziehungsweise fortzuschreiben. Zu diesem Zweck sieht die Verordnung (EU) 2016/679 auch Öffnungsklauseln vor, um nationale Bestimmungen im Zusammenhang mit der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, beizubehalten oder einzuführen.

Gleiches gilt im Hinblick auf die besonderen Verarbeitungssituationen, wie etwa den Beschäftigtendatenschutz, die Datenverarbeitung zu Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken. Schließlich sieht die Verordnung (EU) 2016/679 auch die Möglichkeit der Abweichung von Betroffenenrechten zu bestimmten Zwecken vor. Zur gleichmäßigen Durchsetzung ihrer Ziele enthält die Verordnung (EU) 2016/679 zudem Regelungsaufträge an die Mitgliedstaaten, die vorsehen, dass ihre Bestimmungen unter bestimmten Vorgaben einheitlich umgesetzt werden. Sofern die Verordnung (EU) 2016/679 keine Regelungsoptionen der Mitgliedstaaten vorsieht, gelten ihre Bestimmungen abschließend und unmittelbar. Aufgrund des damit verbundenen Anwendungsvorrangs des Unionsrechts werden nationale Vorschriften im Kollisionsfall verdrängt.

Bis zum 6. Mai 2018 müssen die Mitgliedstaaten darüber hinaus die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) in nationales Recht umsetzen. Anders als bei Verordnungen bleibt es den Mitgliedstaaten grundsätzlich überlassen, wie sie Richtlinien umsetzen (Artikel 288 Abs. 3 des AEU-Vertrages). Sie haben bei der Umsetzung einen gewissen Spielraum. Von diesem Handlungsspielraum wird in Artikel 1 (Thüringer Datenschutzgesetz) und Artikel 4 (Änderung des Polizeiaufgabengesetzes) Gebrauch gemacht.

Die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 erfordern eine Abgrenzung. Es bedarf hierzu der Prüfung im Einzelfall, ob eine Behörde Daten zu den in der Verordnung (EU) 2016/679 oder zu den in der Richtlinie (EU) 2016/680 geregelten Zwecken verarbeitet. Für die in Artikel 1 dieses Gesetzes vorgesehene gemeinsame Umsetzung im Thüringer Datenschutzgesetz (ThürDSG) spricht der Umstand, dass in einer Vielzahl von Fällen Behörden sowohl allgemein verwaltend, als auch im Zusammenhang mit der Verhütung, Ermittlung, Aufdeckung, Verfolgung und Vollstreckung von Straftaten und Ordnungswidrigkeiten oder der Gefahrenabwehr tätig sind. Daher werden im Ersten, Zweiten und Vierten Abschnitt die Verordnung (EU) 2016/679 und im Ersten, Dritten und Vierten Abschnitt die Richtlinie (EU) 2016/680 umgesetzt. Der Fünfte Abschnitt enthält spezielle Bestimmungen für Verarbeitungen, auf welche die Verordnung (EU) 2016/679 nur für entsprechend anwendbar erklärt wurde. Der Sechste Abschnitt enthält Übergangs- und Schlussbestimmungen. Die Frage der Eröffnung des Anwendungsbereichs des jeweiligen Abschnitts des Thüringer Datenschutzgesetzes bestimmt sich also nach dem Zusammenhang im Einzelfall, in dem der Verantwortliche personenbezogene Daten verarbeitet (§ 1 ThürDSG).

Zur Gewährleistung eines reibungslosen Zusammenspiels der aufgezeigten Rechtsregime sind grundlegende Änderungen gegenüber dem bisher geltenden Thüringer Datenschutzgesetz erforderlich, die eine Aufrechterhaltung seiner Struktur ausschließen. Das bisher geltende Thüringer Datenschutzgesetz wird daher aufgehoben.

In dem Artikelgesetz stehen folgende Änderungen im Vordergrund:

- Anpassung des Thüringer Datenschutzgesetzes an die Gliederung und Struktur der Verordnung (EU) 2016/679,
- Streichen der Bestimmungen, die sich nunmehr unmittelbar aus der Verordnung (EU) 2016/679 ergeben,
- Regelung logischer Ergänzungen und Ausnahmen von den Betroffenenrechten nach der Verordnung (EU) 2016/679,
- Nutzung der Öffnungsklauseln der Verordnung (EU) 2016/679 zur Aufrechterhaltung der Regelungen zu besonderen Verarbeitungssituationen,
- Stärkung der Unabhängigkeit des Landesbeauftragten für den Datenschutz,
- Umsetzung der Vorgaben der Richtlinie (EU) 2016/680 in Anlehnung an die Verordnung (EU) 2016/679 und unter Berücksichtigung der besonderen Bedürfnisse der Behördentätigkeit in diesem Bereich,
- Zusammenführung des allgemeinen Datenschutzrechts nach der Verordnung (EU) 2016/679 und des allgemeinen Polizeidatenschutzrechts nach der Richtlinie (EU) 2016/680,
- Umsetzung der Richtlinie (EU) 2016/680 im Polizeiaufgabengesetz sowie
- Anpassung von Datenschutzbezügen im Fachrecht (Artikel 2 bis 26).

B. Lösung

Der Gesetzentwurf sieht mehrere Gesetzesänderungen vor.

In Artikel 1 wird das Thüringer Datenschutzgesetz neu gefasst. Damit soll ein einheitlicher allgemeiner Rechtsrahmen für die Verarbeitung personenbezogener Daten durch alle öffentlichen Stellen gegeben werden, die in den Anwendungsbereich dieses Gesetzes fallen. Dabei wird das allgemeine Datenschutzrecht für öffentliche Stellen sowie im speziellen das allgemeine Datenschutzrecht für die Polizei und andere Behörden der Strafverhütung, -ermittlung, -aufdeckung, -verfolgung und -vollstreckung sowie der Gefahrenabwehr in einem Gesetz zusammengefasst. Grundlage und Ausgangspunkt des neuen allgemeinen materiellen Datenschutzrechts im Ersten Abschnitt sind die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680. In Umsetzung der Richtlinie (EU) 2016/680 gilt daher nicht das Zitierverbot für Verordnungen. Im Zweiten Abschnitt wird ausschließlich die Verordnung (EU) 2016/679 umgesetzt. Das Thüringer Datenschutzgesetz kann daher in diesem Abschnitt unter Berücksichtigung des Zitier- und Wiederholungsverbots (Erwägungsgrund 8) europarechtlich verbindlicher Vorschriften nur ergänzende Regelungen zu einzelnen Vorschriften treffen. Im Dritten Abschnitt wird nunmehr der allgemeine Datenschutz für Polizei und andere Behörden der Strafverhütung, -ermittlung, -aufdeckung, -verfolgung und -vollstreckung sowie der Gefahrenabwehr geregelt. Der Vierte Abschnitt enthält Bestimmungen zu Ordnungswidrigkeiten und Straftatbeständen sowohl im Anwendungsbereich der Verordnung (EU) 2016/679 als auch der Richtlinie (EU) 2016/680. Der Fünfte Abschnitt beinhaltet Ausnahmeregelungen für Verarbeitungssituationen, die europarechtlich nicht vorgeprägt sind und damit nicht dem Anwendungsbereich der Verordnung (EU) 2016/679 oder der Richtlinie (EU) 2016/680 unterfallen, für welche die Verordnung (EU) 2016/679 allerdings für entsprechend anwendbar erklärt wird.

Das neue Thüringer Datenschutzgesetz besteht damit insgesamt aus sechs Abschnitten:

1. Gemeinsame Bestimmungen
 - Zweck und Anwendungsbereich des Gesetzes
 - Regelungen zur Aufsichtsbehörde
 - Regelungen zum Datenschutzbeauftragten
2. Bestimmungen für die Verarbeitung zu Zwecken nach Artikel 2 der Verordnung (EU) 2016/679
 - Rechtsgrundlagen der Verarbeitung
 - Rechte der betroffenen Personen
 - besondere Verarbeitungssituationen
3. Bestimmungen für die Verarbeitung zu Zwecken nach Artikel 1 Abs. 1 der Richtlinie (EU) 2016/680
 - Anwendungsbereich und Grundsätze
 - Begriffsbestimmungen
 - Rechte der betroffenen Personen
 - Pflichten der Verantwortlichen und Auftragsverarbeiter
 - Datensicherheit
 - Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen
4. Ordnungswidrigkeit, Strafbestimmungen
5. Orden und Ehrenzeichen, Gnadensachen
6. Übergangs- und Schlussbestimmungen

Durch Artikel 4 wird die Richtlinie (EU) 2016/680 im Polizeiaufgabengesetz umgesetzt. Die Artikel 2 bis 26 enthalten weitere notwendige Änderungen im Fachrecht.

Artikel 27 bestimmt das Inkrafttreten der neuen und das Außerkrafttreten der bisherigen Regelungen, welches sich nach den unionsrechtlichen Vorgaben bemisst.

C. Alternative

Keine

D. Kosten

Mit der Umsetzung der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 werden dem Landesbeauftragten für den Datenschutz (TLfD) weitere Rechte und Pflichten eingeräumt. Infolge deren Wahrnehmung ergibt sich wahrscheinlich ein Mehrbedarf an Personal. Um wie viele Stellen es sich dabei handelt, kann derzeit nicht abschließend beziffert werden. Jedenfalls aber wurden die entstehenden Mehrkosten bei dem Landesbeauftragten für den Datenschutz im Zuge der Aufstellung des Doppelhaushalts 2018/2019 durch eine Personalmehrung (zwei bereits umgesetzte Planstellen sowie in den Jahren 2018 und 2019 jeweils eine weitere Planstelle) berücksichtigt. Gleichzeitig erfolgt durch bundesgesetzliche Regelung eine Aufgabenerleichterung des Landesbeauftragten für den Datenschutz (§ 32h Abs. 1 Satz 1 der Abgabenordnung in der ab 25. Mai 2018 geltenden Fassung). Der konkrete Personalbedarf und die daraus resultierenden Personal- und Sachkosten beim TLfD können zum jetzigen Zeitpunkt nicht beziffert werden. Sie gehen auf die Bestimmungen der Verordnung (EU) 2016/679 zurück und werden durch diesen Gesetzentwurf weder ausgelöst noch konkretisiert. Entsprechendes gilt für den Bereich der Richtlinie (EU) 2016/680, deren verbindliche Mindeststandards durch diesen Gesetzesentwurf umgesetzt werden.

Weiterhin werden in Folge der Umsetzung der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 Betroffenenrechte gestärkt. Öffentliche Stellen müssen im Umgang mit den Betroffenenrechten daher ihre Verfahren überprüfen und überarbeiten. Zusätzlich sind technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes zu überarbeiten (beispielsweise Datenschutz-Folgenabschätzung, Verzeichnis von Verarbeitungstätigkeiten). Sie gehen ebenfalls auf die Bestimmungen der Verordnung (EU) 2016/679 zurück und werden durch diesen Gesetzentwurf nicht ausgelöst. Schließlich verändert sich die Rolle des behördlichen Datenschutzbeauftragten, dieser wird ein Kerninstrument des Verantwortlichen bei der Einhaltung datenschutzrechtlicher Vorschriften. Durch die vorstehend genannten Maßnahmen entsteht zusätzlicher Aufwand für die Verwaltung, der jedoch in personellem und finanziellem Mehraufwand nicht beziffert werden kann.

E. Zuständigkeit

Federführend ist das Ministerium für Inneres und Kommunales

**FREISTAAT THÜRINGEN
DER MINISTERPRÄSIDENT**

An den
Präsidenten des Thüringer Landtags
Herrn Christian Carius
Jürgen-Fuchs-Straße 1

99096 Erfurt

Erfurt, den 16. Januar 2018

Sehr geehrter Herr Präsident,

hiermit überreiche ich den von der Landesregierung beschlossenen Entwurf des

"Thüringer Gesetzes zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Thüringer Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - ThürDSAnpUG-EU -)"

mit der Bitte um Beratung durch den Landtag in den Plenarsitzungen am 24./25./26. Januar 2018.

Mit freundlichen Grüßen

Bodo Ramelow

**Thüringer Gesetz
zur Anpassung des Allgemeinen Datenschutzrechts an
die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680
(Thüringer Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - ThürDSAnpUG-EU -)**

Inhaltsübersicht

- Artikel 1 Thüringer Datenschutzgesetz (ThürDSG)
- Artikel 2 Änderung des Thüringer Gesetzes über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid
- Artikel 3 Änderung des Ordnungsbehördengesetzes
- Artikel 4 Änderung des Polizeiaufgabengesetzes
- Artikel 5 Änderung des Thüringer Kommunalwahlgesetzes
- Artikel 6 Änderung des Thüringer Beamtengesetzes
- Artikel 7 Änderung des Thüringer Personalvertretungsgesetzes
- Artikel 8 Änderung des Thüringer Informationsfreiheitsgesetzes
- Artikel 9 Änderung des Thüringer Stiftungsgesetzes
- Artikel 10 Änderung des Thüringer Rettungsdienstgesetzes
- Artikel 11 Änderung des Thüringer Vermessungs- und Geoinformationsgesetzes
- Artikel 12 Änderung des Thüringer Hochschulgebühren- und -entgeltgesetzes
- Artikel 13 Änderung des Thüringer Schulgesetzes
- Artikel 14 Änderung des Thüringer Gesetzes zur Ausführung des Artikel 10-Gesetzes
- Artikel 15 Änderung des Thüringer Verfassungsschutzgesetzes
- Artikel 16 Änderung des Thüringer Sicherheitsüberprüfungsgesetzes
- Artikel 17 Änderung des Thüringer Statistikgesetzes
- Artikel 18 Änderung des Thüringer Gesetzes zur Ausführung der Verwaltungsgerichtsordnung
- Artikel 19 Änderung des Thüringer Gesetzes zur Umsetzung der Bestimmungen über die europäische Amtshilfe
- Artikel 20 Änderung des Thüringer Tiergesundheitsgesetzes
- Artikel 21 Änderung des Thüringer Landesmediengesetzes
- Artikel 22 Änderung des Thüringer Pressegesetzes
- Artikel 23 Änderung des Gesetzes über das Verfahren bei Einwohnerantrag, Bürgerbegehren und Bürgerentscheid
- Artikel 24 Änderung des Thüringer Berufsqualifikationsfeststellungsgesetzes
- Artikel 25 Änderung des Thüringer Bestattungsgesetzes
- Artikel 26 Änderung des Thüringer Laufbahngesetzes
- Artikel 27 Inkrafttreten, Außerkrafttreten

Der Landtag hat das folgende Gesetz beschlossen:

Artikel 1
Thüringer Datenschutzgesetz (ThürDSG)

Inhaltsübersicht

Erster Abschnitt
Gemeinsame Bestimmungen

Erster Unterabschnitt
Allgemeine Bestimmungen

- § 1 Zweck des Gesetzes
- § 2 Anwendungsbereich

Zweiter Unterabschnitt
Aufsichtsbehörde

- § 3 Landesbeauftragter für den Datenschutz (Artikel 51 bis 54 der Verordnung (EU) 2016/679, Artikel 41 bis 44 der Richtlinie (EU) 2016/680)
- § 4 Rechtsstellung und Verschwiegenheitspflicht des Landesbeauftragten für den Datenschutz (Artikel 51 bis 54 der Verordnung (EU) 2016/679, Artikel 41 bis 44 der Richtlinie (EU) 2016/680)
- § 5 Anwendung beamtenrechtlicher Vorschriften auf den Landesbeauftragten für den Datenschutz
- § 6 Aufgaben des Landesbeauftragten für den Datenschutz (Artikel 57 und 31 der Verordnung (EU) 2016/679, Artikel 46 und 26 der Richtlinie (EU) 2016/680)
- § 7 Befugnisse des Landesbeauftragten für den Datenschutz (Artikel 58 und 83 der Verordnung (EU) 2016/679, Artikel 47 der Richtlinie (EU) 2016/680)
- § 8 Anrufung des Landesbeauftragten für den Datenschutz (Artikel 77 der Verordnung (EU) 2016/679, Artikel 52 der Richtlinie (EU) 2016/680)
- § 9 Rechtsschutz gegen Anordnungen des Landesbeauftragten für den Datenschutz oder bei dessen Untätigkeit (Artikel 78 der Verordnung (EU) 2016/679, Artikel 53 der Richtlinie (EU) 2016/680)
- § 10 Weitere Aufgaben des Landesbeauftragten für den Datenschutz (Artikel 59 der Verordnung (EU) 2016/679, Artikel 49 der Richtlinie (EU) 2016/680)
- § 11 Aufsichtsbehörde gegenüber nichtöffentlichen Stellen und öffentlichen Stellen, die am Wettbewerb teilnehmen
- § 12 Beirat

Dritter Unterabschnitt
Datenschutzbeauftragter

- § 13 Bestellung des Datenschutzbeauftragten (Artikel 37 der Verordnung (EU) 2016/679, Artikel 32 der Richtlinie (EU) 2016/680)
- § 14 Stellung des Datenschutzbeauftragten (Artikel 38 der Verordnung (EU) 2016/679, Artikel 33 der Richtlinie (EU) 2016/680)
- § 15 Aufgaben des Datenschutzbeauftragten (Artikel 39 der Verordnung (EU) 2016/679, Artikel 34 der Richtlinie (EU) 2016/680)

Zweiter Abschnitt
Bestimmungen für die Verarbeitung zu Zwecken
nach Artikel 2 der Verordnung (EU) 2016/679

Erster Unterabschnitt
Rechtsgrundlagen der Verarbeitung

- § 16 Verarbeitung personenbezogener Daten (Artikel 6 und 9 der Verordnung (EU) 2016/679)
- § 17 Zweckbindung und Zulässigkeit der Weiterverarbeitung (Artikel 6 und 23 der Verordnung (EU) 2016/679)
- § 18 Übermittlung (Artikel 6 Abs. 2 der Verordnung (EU) 2016/679)
- § 19 Auftragsverarbeitung (Artikel 28 der Verordnung (EU) 2016/679)

Zweiter Unterabschnitt
Rechte der betroffenen Personen

- § 20 Informationspflichten (Artikel 13, 14 und 23 der Verordnung (EU) 2016/679)
- § 21 Auskunftsrecht (Artikel 15 und 23 der Verordnung (EU) 2016/679)
- § 22 Recht auf Einschränkung der Verarbeitung (Artikel 18 der Verordnung (EU) 2016/679)
- § 23 Löschung personenbezogener Daten (Artikel 17 der Verordnung (EU) 2016/679)
- § 24 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Artikel 34 der Verordnung (EU) 2016/679)

Dritter Unterabschnitt
Besondere Verarbeitungssituationen

- § 25 Verarbeitung personenbezogener Daten zu Zwecken der freien Meinungsäußerung und der Informationsfreiheit
- § 26 Öffentliche Stellen, die am Wettbewerb teilnehmen
- § 27 Datenschutz im Beschäftigungskontext (Artikel 88 der Verordnung (EU) 2016/679)
- § 28 Verarbeitung personenbezogener Daten durch Forschungseinrichtungen (Artikel 6, 9 und 89 der Verordnung (EU) 2016/679)
- § 29 Zweckbindung von personenbezogenen Daten, die einem Berufsgeheimnis unterliegen (Artikel 6 und 9 der Verordnung (EU) 2016/679)
- § 30 Videoüberwachung

Dritter Abschnitt
Bestimmungen für Verarbeitungen zu Zwecken
nach Artikel 1 Abs. 1 der Richtlinie (EU) 2016/680

Erster Unterabschnitt
Anwendungsbereich und Grundsätze

- § 31 Anwendungsbereich (Artikel 1 Abs. 1, Artikel 2 Abs. 1 der Richtlinie (EU) 2016/680)
- § 32 Begriffsbestimmungen (Artikel 3 der Richtlinie (EU) 2016/680)
- § 33 Grundsätze bei der Verarbeitung personenbezogener Daten (Artikel 8, Artikel 4 Abs. 2 und 3, Artikel 9 Abs. 2 und 3 der Richtlinie (EU) 2016/680)

- § 34 Unterscheidung verschiedener Kategorien betroffener Personen sowie zwischen Tatsachen und Bewertungen (Artikel 6, Artikel 7 Abs. 1 der Richtlinie (EU) 2016/680)
- § 35 Berichtigung und Löschung personenbezogener Daten sowie die Einschränkung der Verarbeitung (Artikel 4 Abs. 1, Artikel 7 Abs. 3, Artikel 5 der Richtlinie (EU) 2016/680)
- § 36 Verfahren bei Übermittlungen (Artikel 7 Abs. 2, Artikel 9 Abs. 3 und 4 der Richtlinie (EU) 2016/680)
- § 37 Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 10 der Richtlinie (EU) 2016/680)
- § 38 Automatisierte Einzelentscheidung (Artikel 11 der Richtlinie (EU) 2016/680)
- § 39 Einwilligung

**Zweiter Unterabschnitt
Rechte der betroffenen Person**

- § 40 Allgemeiner Informationsanspruch (Artikel 13 Abs. 1 der Richtlinie (EU) 2016/680)
- § 41 Benachrichtigung betroffener Personen (Artikel 13 Abs. 2 und 3 der Richtlinie (EU) 2016/680)
- § 42 Auskunftsrecht (Artikel 14 bis 17 der Richtlinie (EU) 2016/680)
- § 43 Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung (Artikel 16 der Richtlinie (EU) 2016/680)
- § 44 Verfahren für die Ausübung der Rechte der betroffenen Person (Artikel 12 Abs. 1 und 3 bis 5 der Richtlinie (EU) 2016/680)
- § 45 Schadensersatz (Artikel 56 der Richtlinie (EU) 2016/680)

**Dritter Unterabschnitt
Pflichten der Verantwortlichen und
Auftragsverarbeiter**

- § 46 Pflichten des Verantwortlichen (Artikel 20 der Richtlinie (EU) 2016/680)
- § 47 Gemeinsam Verantwortliche (Artikel 21 der Richtlinie (EU) 2016/680)
- § 48 Auftragsverarbeitung (Artikel 22 der Richtlinie (EU) 2016/680)
- § 49 Verarbeitung auf Weisung, Datengeheimnis (Artikel 23 der Richtlinie (EU) 2016/680)
- § 50 Verzeichnis von Verarbeitungstätigkeiten (Artikel 24 der Richtlinie (EU) 2016/680)
- § 51 Protokollierung (Artikel 25 der Richtlinie (EU) 2016/680)
- § 52 Durchführung einer Datenschutz-Folgenabschätzung (Artikel 27 der Richtlinie (EU) 2016/680)
- § 53 Anhörung des Landesbeauftragten für den Datenschutz (Artikel 28 der Richtlinie (EU) 2016/680)

**Vierter Unterabschnitt
Datensicherheit**

- § 54 Anforderungen an die Sicherheit der Datenverarbeitung (Artikel 29 der Richtlinie (EU) 2016/680)
- § 55 Meldung von Verletzungen des Schutzes personenbezogener Daten an den Landesbeauftragten für den Datenschutz (Artikel 30 der Richtlinie (EU) 2016/680)

- § 56 Benachrichtigung der betroffenen Person bei Verletzungen des Schutzes personenbezogener Daten (Artikel 31 der Richtlinie (EU) 2016/680)

Fünfter Unterabschnitt

Übermittlung personenbezogener Daten an Drittstaaten oder internationale Organisationen

- § 57 Allgemeine Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten und internationale Organisationen (Artikel 35 und 36 der Richtlinie (EU) 2016/680)
- § 58 Datenübermittlung bei geeigneten Garantien (Artikel 37 der Richtlinie (EU) 2016/680)
- § 59 Datenübermittlung ohne Angemessenheitsbeschluss und ohne geeignete Garantien (Artikel 38 der Richtlinie (EU) 2016/680)
- § 60 Sonstige Datenübermittlung an Empfänger in Drittstaaten (Artikel 39 der Richtlinie (EU) 2016/680)

Vierter Abschnitt

Ordnungswidrigkeiten und Strafbestimmungen

- § 61 Ordnungswidrigkeiten und Strafbestimmungen

Fünfter Abschnitt

Orden und Ehrenzeichen, Gnadensachen

- § 62 Orden und Ehrenzeichen
- § 63 Gnadensachen

Sechster Abschnitt

Übergangs- und Schlussbestimmungen

- § 64 Übergangsbestimmungen
- § 65 Gleichstellungsbestimmung

Erster Abschnitt

Gemeinsame Bestimmungen

Erster Unterabschnitt

Allgemeine Bestimmungen

§ 1

Zweck des Gesetzes

(1) Dieses Gesetz trifft in dem Ersten, Zweiten und Vierten Abschnitt ergänzende Regelungen zur Durchführung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72).

(2) Dieses Gesetz dient in dem Ersten, Dritten und Vierten Abschnitt der Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Straf-

verfolgung und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89). Die weitere Umsetzung der Richtlinie (EU) 2016/680 obliegt dem jeweiligen Fachgesetz.

§ 2 Anwendungsbereich

(1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch die Behörden, die Gerichte und die sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände und die sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts (öffentliche Stellen).

(2) Als öffentliche Stellen gelten auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts beteiligt sind. Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts, auf die dieses Gesetz nach Satz 1 Anwendung findet, an einer weiteren Vereinigung des privaten Rechts, so findet Satz 1 entsprechende Anwendung. Nehmen nichtöffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr, sind sie insoweit öffentliche Stellen im Sinne dieses Gesetzes.

(3) Nicht als öffentliche Stellen nach Absatz 1 gelten öffentlich-rechtliche Kreditinstitute und öffentlich-rechtliche Versicherungsanstalten und deren Verbände. Auf sie finden die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) vom 30. Juni 2017 (BGBl. I S. 2097) in der jeweils geltenden Fassung über nichtöffentliche Stellen Anwendung, es sei denn, durch Gesetz oder Staatsvertrag ist ausdrücklich die Anwendung dieses Gesetzes oder des Datenschutzgesetzes eines anderen Landes bestimmt.

(4) Soweit besondere Rechtsvorschriften über den Datenschutz auf personenbezogene Daten anzuwenden sind, gehen sie den Bestimmungen dieses Gesetzes vor. Regeln diese Rechtsvorschriften einen Sachverhalt nicht oder nicht abschließend, finden die Bestimmungen dieses Gesetzes Anwendung. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(5) Fällt die Verarbeitung personenbezogener Daten nicht in den Anwendungsbereich der Verordnung (EU) 2016/679 oder der in Umsetzung der Richtlinie (EU) 2016/680 getroffenen Regelungen, sind die Bestimmungen der Verordnung (EU) 2016/679 entsprechend anzuwenden, es sei denn, dieses Gesetz oder die jeweiligen Fachgesetze enthalten abweichende Regelungen. Satz 1 gilt mit Ausnahme der Artikel 30, 35 und 36 der Verordnung (EU) 2016/679 auch für die nichtautomatisierte Verarbeitung personenbezogener Daten, die nicht in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

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

(7) Die Bestimmungen dieses Gesetzes gelten für den Landtag nur, soweit er in Verwaltungsangelegenheiten tätig wird. Verwaltungsangelegenheiten des Landtags sind insbesondere

1. die wirtschaftlichen Angelegenheiten des Landtags nach Artikel 57 Abs. 4 Satz 1 der Verfassung des Freistaats Thüringen,
2. die Personalverwaltung des Landtags,
3. die Ausübung des Hausrechts und der Ordnungs- und Polizeigewalt nach Artikel 57 Abs. 3 Satz 2 der Verfassung des Freistaats Thüringen und
4. die Ausführung der Gesetze, soweit diese dem Präsidenten des Landtags zugewiesen sind und nicht in unmittelbarem Zusammenhang mit der Wahrnehmung parlamentarischer Aufgaben stehen.

Für die Verarbeitung personenbezogener Daten bei der Wahrnehmung parlamentarischer Aufgaben durch den Landtag einschließlich der Fraktionen finden die Bestimmungen dieses Gesetzes unter Berücksichtigung der verfassungsrechtlichen Stellung des Landtags entsprechende Anwendung. Soweit der Landtag in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeitet, wird die Einhaltung des Datenschutzes durch den Ältestenrat des Landtags kontrolliert.

(8) Für den Rechnungshof gelten die Bestimmungen über die Aufsichtsbehörde, den Datenschutzbeauftragten sowie das Führen von Verzeichnissen nach Artikel 30 der Verordnung (EU) 2016/679 nur, soweit er in Verwaltungsangelegenheiten tätig wird. Für die Gerichte gilt Satz 1 entsprechend mit der Maßgabe, dass § 50 auch bei Verarbeitungstätigkeiten, die in Zusammenhang mit der Mitwirkung an der Strafverfolgung, der Verfolgung von Ordnungswidrigkeiten und der Vollstreckung stehen, keine Anwendung findet.

(9) Bei der im Anwendungsbereich des § 31 geregelten Verarbeitung personenbezogener Daten gelten für die Staatsanwaltschaften die Bestimmungen des Ersten, Dritten und Vierten Abschnitts, im Übrigen gelten für sie die Bestimmungen des Ersten, Zweiten und Vierten Abschnitts.

Zweiter Unterabschnitt Aufsichtsbehörde

§ 3

Landesbeauftragter für den Datenschutz
(Artikel 51 bis 54 der Verordnung (EU) 2016/679,
Artikel 41 bis 44 der Richtlinie (EU) 2016/680)

(1) Der Landtag wählt den Landesbeauftragten für den Datenschutz mit mehr als der Hälfte der gesetzlichen Anzahl seiner Mitglieder. Der Gewählte ist vom Präsidenten des Landtags zu ernennen. Das Amtsverhältnis beginnt mit der Aushändigung der Ernennungsurkunde.

(2) Der Landesbeauftragte für den Datenschutz muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich des Schutzes personenbezogener Daten verfügen; insbesondere muss der Landesbeauftragte für den Datenschutz über durch einschlägige Berufserfahrung erworbene Kenntnisse des Datenschutzrechts verfügen.

(3) Der Landesbeauftragte für den Datenschutz steht zum Land in einem öffentlich-rechtlichen Amtsverhältnis.

(4) Die Amtszeit des Landesbeauftragten für den Datenschutz beträgt sechs Jahre. Einmalige Wiederwahl ist zulässig.

(5) Der Präsident des Landtags verpflichtet den Landesbeauftragten für den Datenschutz vor dem Landtag, sein Amt gerecht und unparteiisch zu führen, das Grundgesetz und die Verfassung des Freistaats Thüringen sowie die Gesetze zu wahren und zu verteidigen. Der Landesbeauftragte für den Datenschutz leistet vor dem Präsidenten des Landtags folgenden Eid: "Ich schwöre, mein Amt gerecht und unparteiisch getreu dem Grundgesetz, der Verfassung des Freistaats Thüringen und den Gesetzen zu führen und meine ganze Kraft dafür einzusetzen, so wahr mir Gott helfe." Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(6) Auf Vorschlag des Landesbeauftragten für den Datenschutz ernennt der Präsident des Landtags einen Vertreter im Amt. Dieser soll die Befähigung zum Richteramt haben.

(7) Dienstsitz des Landesbeauftragten für den Datenschutz ist Erfurt.

(8) Das Amtsverhältnis endet mit Ablauf der Amtszeit, mit Rücktritt oder verpflichtender Versetzung in den Ruhestand. Der Präsident des Landtags entlässt den Landesbeauftragten für den Datenschutz, wenn er eine schwere Verfehlung begangen hat oder er die Voraussetzungen für die Wahrnehmung seiner Aufgabe nicht mehr erfüllt. Bei Beendigung des Amtsverhältnisses erhält der Landesbeauftragte für den Datenschutz eine vom Präsidenten des Landtags unterzeichnete Urkunde. Die Entlassung wird mit der Aushändigung der Urkunde durch den Präsidenten des Landtags wirksam.

(9) Endet das Amtsverhältnis mit Ablauf der Amtszeit, ist der Landesbeauftragte für den Datenschutz verpflichtet, die Geschäfte bis zur Ernennung eines Nachfolgers für die Dauer von höchstens sechs Monaten fortzuführen; Absatz 8 Satz 2 gilt für diesen Zeitraum entsprechend.

§ 4

Rechtsstellung und Verschwiegenheitspflicht
des Landesbeauftragten für den Datenschutz
(Artikel 51 bis 54 der Verordnung (EU) 2016/679,
Artikel 41 bis 44 der Richtlinie (EU) 2016/680)

(1) Der Landesbeauftragte für den Datenschutz ist Aufsichtsbehörde nach Artikel 51 der Verordnung (EU) 2016/679 und zugleich Aufsichtsbehörde im Sinne des Artikels 41 der Richtlinie (EU) 2016/680.

(2) Der Landesbeauftragte für den Datenschutz sieht von allen mit den Aufgaben seines Amtes nicht zu vereinbarenden Handlungen ab und übt während seiner Amtszeit keine andere mit seinem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus. Er darf insbesondere kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens als Mitglied angehören.

teten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) Der Landesbeauftragte für den Datenschutz sowie seine Mitarbeiter sind sowohl während ihrer Amts- beziehungsweise Dienstzeit als auch nach deren Beendigung verpflichtet, über alle vertraulichen Informationen, die ihnen bei der Wahrnehmung ihrer Aufgaben oder der Ausübung ihrer Befugnisse bekannt geworden sind, Verschwiegenheit zu wahren.

(4) Die Verschwiegenheitspflicht nach Absatz 3 gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

(5) Der Landesbeauftragte für den Datenschutz ist oberste Dienstbehörde im Sinne des § 96 der Strafprozessordnung sowie oberste Aufsichtsbehörde im Sinne des § 99 der Verwaltungsgerichtsordnung. Er trifft die Entscheidungen über Aussagegenehmigungen für sich und seine Mitarbeiter sowie die Entscheidung über die Verweigerung der Aktenvorlage und der Auskunftserteilung in eigener Verantwortung. Der Nachfolger im Amt entscheidet über die in Satz 2 genannten Entscheidungen für seine Vorgänger.

(6) Dem Landesbeauftragten für den Datenschutz sind die für die Erfüllung seiner Aufgaben und Befugnisse nötige personelle, technische, finanzielle Ausstattung sowie Räumlichkeiten und Infrastruktur zur Verfügung zu stellen; entsprechende Haushaltsmittel sind im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen. Er untersteht der Finanzkontrolle durch den Rechnungshof nur, soweit seine Unabhängigkeit dadurch nicht beeinträchtigt wird.

(7) Die Besetzung der Personalstellen kann nur auf Vorschlag des Landesbeauftragten für den Datenschutz erfolgen. Seine Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur mit seinem Einvernehmen versetzt, abgeordnet oder umgesetzt werden; er ist ihr Dienstvorgesetzter, sie sind in ihrer Tätigkeit nach diesem Gesetz nur an seine Weisungen gebunden.

§ 5

Anwendung beamtenrechtlicher Vorschriften auf den Landesbeauftragten für den Datenschutz

(1) Der Landesbeauftragte für den Datenschutz erhält ab dem Tage seiner Ernennung bis zum Ablauf des Tages der Beendigung seines Amtsverhältnisses, im Fall des § 3 Abs. 9 bis zum Ablauf des Tages, an dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Landesbeamten der Besoldungsgruppe B 6 in Thüringen jeweils zustehenden Besoldung.

(2) Der Landesbeauftragte für den Datenschutz erhält Reisekosten, Umzugskosten, Trennungsgeld und Beihilfen nach den für die Landesbeamten geltenden Vorschriften. Gleiches gilt für die Unfallfürsorge und in Urlaubsanlässen.

(3) Der Landesbeauftragte für den Datenschutz oder seine Hinterbliebenen erhalten nach Beendigung seines Amtsverhältnisses, im Fall des § 3 Abs. 9 nach Ablauf des Tages, an dem die Geschäftsführung endet, Versorgung wie ein Beamter auf Zeit in entsprechender Anwendung des Thüringer Beamtenversorgungsgesetzes. Der Anspruch auf Ruhegehalt ruht bis zum Erreichen der Altersgrenze nach § 25 Abs. 1 oder 3 des Thüringer Beamtengesetzes (ThürBG).

§ 6

Aufgaben des Landesbeauftragten für den Datenschutz
(Artikel 57 und 31 der Verordnung (EU) 2016/679,
Artikel 46 und 26 der Richtlinie (EU) 2016/680)

(1) Der Landesbeauftragte für den Datenschutz nimmt gegenüber den öffentlichen Stellen des Landes die Aufgaben nach Artikel 57 der Verordnung (EU) 2016/679 wahr. Dabei kontrolliert er die Einhaltung der Verordnung (EU) 2016/679, dieses Gesetzes sowie anderer datenschutzrechtlicher Bestimmungen.

(2) Unbeschadet von Absatz 1 hat der Landesbeauftragte für den Datenschutz im Rahmen von Verarbeitungstätigkeiten im Anwendungsbereich der Richtlinie (EU) 2016/680 die Aufgaben,

1. die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschließlich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zu überwachen und durchzusetzen,
2. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären, wobei spezifische Maßnahmen für Minderjährige besondere Beachtung finden,
3. den Landtag, die Landesregierung 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 den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, entstehenden Pflichten 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) 2016/680 erlassenen Rechtsvorschriften, zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten der Europäischen Union zusammenzuarbeiten,
6. sich mit Beschwerden einer betroffenen Person nach § 8 oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes nach Artikel 55 der Richtlinie (EU) 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) 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) 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 der Verwaltungspraktiken,
10. Beratung in Bezug auf die in § 52 genannten Verarbeitungsvorgänge zu leisten und
11. Beiträge zur Tätigkeit des Ausschusses im Sinne des Artikels 51 der Richtlinie (EU) 2016/680 zu leisten.

(3) Verantwortlicher und Auftragsverarbeiter arbeiten auf Anfrage des Landesbeauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben mit diesem zusammen.

§ 7

Befugnisse des Landesbeauftragten für den Datenschutz
(Artikel 58 und 83 der Verordnung (EU) 2016/679,
Artikel 47 der Richtlinie (EU) 2016/680)

(1) Dem Landesbeauftragten für den Datenschutz stehen zur Wahrnehmung der Aufgaben nach § 6 Abs. 1 die Befugnisse nach Artikel 58 der Verordnung (EU) 2016/679 zur Verfügung. Kommt der Landesbeauftragte für den Datenschutz zu dem Ergebnis, dass Verstöße gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt er dies dem Verantwortlichen vor Ausübung seiner Befugnisse nach Artikel 58 Abs. 2 der Verordnung (EU) 2016/679 mit und fordert diesen binnen angemessener Frist zur Stellungnahme auf. Die zuständige oberste Landesbehörde und die Aufsichtsbehörde sind davon zu verständigen. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Mitteilungen getroffen worden sind. Der Landesbeauftragte für den Datenschutz kann auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(2) Dem Landesbeauftragten ist im Rahmen der Kontrollbefugnis jederzeit Zutritt zu allen Diensträumen und Geschäftsräumen zu gewähren. Die Befugnis zur Verhängung von Geldbußen nach Artikel 83 der Verordnung (EU) 2016/679 steht ihm nicht gegenüber öffentlichen Stellen nach § 2 Abs. 1 und 2 zu, es sei denn, es handelt sich um öffentliche Stellen, die am Wettbewerb im Sinne des § 26 teilnehmen.

(3) Die Kontrolle des Landesbeauftragten für den Datenschutz erstreckt sich auch auf personenbezogene Daten, die einem Berufsgeheimnis unterliegen. Für personenbe-

zogene Daten in Akten über die Sicherheitsüberprüfung gilt dies jedoch nur, wenn die betroffene Person der Kontrolle der auf sie bezogenen Daten nicht widersprochen hat. Unbeschadet des Kontrollrechts des Landesbeauftragten für den Datenschutz unterrichtet der Verantwortliche die betroffene Person in allgemeiner Form über das ihr zustehende Widerspruchsrecht. Der Widerspruch ist schriftlich gegenüber dem Verantwortlichen zu erklären.

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

(5) Die in § 21 Abs. 3 genannten öffentlichen Stellen haben eine Pflicht zur Unterstützung des Landesbeauftragten für den Datenschutz nur gegenüber diesem selbst und den von ihm schriftlich besonders damit Beauftragten. Die Pflicht zur Information und zum Zutritt zu Dienstgebäuden findet auf diese Stellen keine Anwendung, soweit die zuständige oberste Landesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht in Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährden würde.

(6) Stellt der Landesbeauftragte für den Datenschutz bei der Verarbeitung personenbezogener Daten, die nicht im Anwendungsbereich der Verordnung (EU) 2016/679 erfolgt, Verstöße gegen die Vorschriften des Datenschutzes fest, so beanstandet er dies gegenüber dem Verantwortlichen und fordert diesen zur Stellungnahme innerhalb einer angemessenen Frist auf. Die zuständige oberste Landesbehörde und die Aufsichtsbehörde sind davon zu verständigen. Der Landesbeauftragte für den Datenschutz kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Beanstandung getroffen worden sind. Wird die Beanstandung nicht behoben, so fordert der Landesbeauftragte von der obersten Landesbehörde und der Aufsichtsbehörde binnen angemessener Frist geeignete Maßnahmen. Hat das nach Ablauf dieser Frist keinen Erfolg, verständigt der Landesbeauftragte den Landtag und die Landesregierung. Der Landesbeauftragte für den Datenschutz 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.

§ 8

Anrufung des Landesbeauftragten für den Datenschutz
(Artikel 77 der Verordnung (EU) 2016/679,
Artikel 52 der Richtlinie (EU) 2016/680)

(1) Jede betroffene Person kann sich unbeschadet eines anderweitigen verwaltungsrechtlichen oder gerichtlichen

Rechtsbehelfs mit einer Beschwerde unmittelbar an den Landesbeauftragten für den Datenschutz wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen des Landes in ihren Rechten verletzt worden zu sein. Der Landesbeauftragte für den Datenschutz hat die betroffene Person über den Stand und das Ergebnis der Beschwerde zu unterrichten und sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes nach § 9 hinzuweisen.

(2) Niemand darf benachteiligt oder gemäßregelt werden, weil er von seinem Recht nach Absatz 1 Gebrauch gemacht hat.

(3) Wendet sich eine betroffene Person an den Landesbeauftragten für den Datenschutz, weil ihr nach § 21 Abs. 5 oder besonderen gesetzlichen Vorschriften keine Auskunft erteilt worden ist, darf die Mitteilung des Landesbeauftragten für den Datenschutz an die betroffene Person keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern diese nicht einer weiter gehenden Auskunft zustimmt. Das Gleiche gilt, wenn eine betroffene Person unmittelbar den Landesbeauftragten für den Datenschutz anruft und die für die Erteilung der Auskunft zuständige Stelle diesem unter Angabe von Gründen darlegt, dass sie bei einem Auskunftersuchen eine Auskunft nach den in Satz 1 genannten Vorschriften verweigern würde.

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

§ 9

Rechtsschutz gegen Anordnungen des Landesbeauftragten für den Datenschutz oder bei dessen Untätigkeit
(Artikel 78 der Verordnung (EU) 2016/679,
Artikel 53 der Richtlinie (EU) 2016/680)

(1) Für Streitigkeiten zwischen öffentlichen Stellen und dem Landesbeauftragten für den Datenschutz über Rechte nach Artikel 78 Abs. 1 und 2 der Verordnung (EU) 2016/679 sowie § 7 Abs. 6 ist der Verwaltungsrechtsweg eröffnet. Bei Verfahren nach Satz 1 gilt § 20 Abs. 2 bis 7 BDSG entsprechend.

(2) Absatz 1 gilt entsprechend zugunsten betroffener Personen, wenn sich der Landesbeauftragte für den Datenschutz nicht mit einer Beschwerde nach § 8 befasst oder die betroffene Person nicht innerhalb von drei Monaten über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.

§ 10

Weitere Aufgaben des Landesbeauftragten für
den Datenschutz
(Artikel 59 der Verordnung (EU) 2016/679,
Artikel 49 der Richtlinie (EU) 2016/680)

(1) Der Landesbeauftragte für den Datenschutz erstellt einen Jahresbericht zu seiner Tätigkeit nach Artikel 59 der

Verordnung (EU) 2016/679 und Artikel 49 der Richtlinie (EU) 2016/680. Dieser ist als elektronisches Dokument zu veröffentlichen und dem Landtag und der Landesregierung elektronisch zu übermitteln.

(2) Der Ministerpräsident führt eine Stellungnahme der Landesregierung zu dem Bericht nach Absatz 1 herbei und legt diese innerhalb von vier Monaten dem Landtag vor.

(3) Der Bericht nach Absatz 1 ist im Beirat beim Landesbeauftragten für den Datenschutz vorzubereiten.

(4) Der Landtag oder die Landesregierung können den Landesbeauftragten für den Datenschutz unbeschadet seiner Unabhängigkeit ersuchen,

1. zu datenschutzrechtlichen Fragen Gutachten zu erstellen und Berichte zu erstatten oder
2. datenschutzrechtliche Vorgänge aus ihrem Aufgabebereich zu überprüfen.

§ 11

Aufsichtsbehörde gegenüber nichtöffentlichen Stellen und öffentlichen Stellen, die am Wettbewerb teilnehmen

(1) Der Landesbeauftragte für den Datenschutz ist auch Aufsichtsbehörde im Sinne des § 40 Abs. 1 BDSG für die Überwachung der Vorschriften über den Datenschutz im Anwendungsbereich der Verordnung EU 2016/679 bei den nichtöffentlichen Stellen und öffentlichen Stellen, die am Wettbewerb teilnehmen.

(2) Zeitgleich mit dem Bericht nach § 10 Abs. 1 legt der Landesbeauftragte für den Datenschutz den Tätigkeitsbericht zu seiner Tätigkeit nach Absatz 1 vor.

§ 12

Beirat

(1) Beim Landesbeauftragten für den Datenschutz wird ein Beirat gebildet. Er besteht aus neun Mitgliedern. Es bestellen sechs Mitglieder der Landtag, ein Mitglied die Landesregierung, ein Mitglied die kommunalen Spitzenverbände sowie ein Mitglied das für Soziales zuständige Ministerium aus dem Bereich der gesetzlichen Sozialversicherungsträger. Für jedes Beiratsmitglied wird zugleich ein Stellvertreter bestellt.

(2) Die Mitglieder des Landtags werden für die Wahldauer des Landtags und die übrigen Mitglieder für vier Jahre bestellt. Sie sind in ihrer Tätigkeit als Mitglieder des Beirats an Aufträge und Weisungen nicht gebunden.

(3) Der Beirat unterstützt den Landesbeauftragten für den Datenschutz in seiner Arbeit. Die Unabhängigkeit des Landesbeauftragten für den Datenschutz und die Berichtspflicht gegenüber dem Landtag werden dadurch nicht berührt.

(4) Der Beirat gibt sich eine Geschäftsordnung. Er tritt auf Antrag jedes seiner Mitglieder oder des Landesbeauftragten für den Datenschutz zusammen. Den Vorsitz führt ein Mitglied des Beirats aus dem Kreis der Landtagsabgeordneten.

(5) Der Landesbeauftragte für den Datenschutz kann an allen Sitzungen teilnehmen. Der Vorsitzende des Beirats lädt ihn zu den Sitzungen rechtzeitig unter Mitteilung der Tagesordnung ein. Vor Maßnahmen, die der Landesbeauftragte für den Datenschutz im Rahmen von § 7 ergreift, kann dem Beirat Gelegenheit zur Stellungnahme gegeben werden.

(6) Die Mitglieder des Beirats haben, auch nach ihrem Ausscheiden, über die ihnen bei ihrer Tätigkeit bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen.

Dritter Unterabschnitt Datenschutzbeauftragter

§ 13

Bestellung des Datenschutzbeauftragten
(Artikel 37 der Verordnung (EU) 2016/679,
Artikel 32 der Richtlinie (EU) 2016/680)

(1) Öffentliche Stellen bestellen einen Datenschutzbeauftragten.

(2) Die öffentliche Stelle kann neben dem Datenschutzbeauftragten zusätzlich weitere Vertreter bestellen. Die Absätze 3 bis 6 sowie die §§ 14 und 15 sind auf die Vertreter nach Satz 1 entsprechend anwendbar.

(3) Der Datenschutzbeauftragte wird für die Dauer von vier Jahren bestellt; Wiederbestellungen sind möglich.

(4) Für mehrere öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter bestellt werden.

(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere seines Fachwissens, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in § 15 genannten Aufgaben bestellt.

(6) Der Datenschutzbeauftragte kann Beschäftigter der öffentlichen Stelle sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

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

§ 14

Stellung des Datenschutzbeauftragten
(Artikel 38 der Verordnung (EU) 2016/679,
Artikel 33 der Richtlinie (EU) 2016/680)

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

(2) Die öffentliche Stelle unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben nach § 15, indem sie die für die Erfüllung dieser Aufgaben erforder-

lichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

(3) Die öffentliche Stelle stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte ist in seiner Funktion dem Leiter der öffentlichen Stelle unmittelbar unterstellt und ist diesem gegenüber berichtspflichtig. Der Datenschutzbeauftragte darf von der öffentlichen Stelle wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden.

(4) Die Abberufung des Datenschutzbeauftragten ist nur in entsprechender Anwendung des § 626 des Bürgerlichen Gesetzbuchs (BGB) zulässig. Die Kündigung des Arbeitsverhältnisses ist unzulässig, es sei denn, dass Tatsachen vorliegen, welche die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach dem Ende der Tätigkeit als Datenschutzbeauftragter ist die Kündigung des Arbeitsverhältnisses innerhalb eines Jahres unzulässig, es sei denn, dass die öffentliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist.

(5) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte nach diesem Gesetz sowie anderen Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen.

(6) Der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über die Umstände, die Rückschlüsse auf sie zulassen, verpflichtet, soweit er hiervon nicht durch die betroffene Person befreit wird. Dies gilt auch nach Beendigung der Tätigkeit als Datenschutzbeauftragter.

(7) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Die öffentliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen und dem Datenschutzbeauftragten für die Erfüllung der Aufgaben nach § 15 hinreichend Arbeitszeit verbleibt.

§ 15

Aufgaben des Datenschutzbeauftragten
(Artikel 39 der Verordnung (EU) 2016/679,
Artikel 34 der Richtlinie (EU) 2016/680)

(1) Der Datenschutzbeauftragte nimmt die Aufgaben nach Artikel 39 der Verordnung (EU) 2016/679 wahr. Dabei kontrolliert er die Einhaltung der Verordnung (EU) 2016/679, dieses Gesetzes sowie anderer datenschutzrechtlicher Bestimmungen.

(2) Der Datenschutzbeauftragte hat das Recht auf Einsichtnahme in das Verzeichnis aller Verarbeitungstätigkeiten. Vor erstmaliger Inbetriebnahme einer Verarbeitungstätigkeit ist dem Datenschutzbeauftragten das Verzeichnis mit der Gelegenheit zur Stellungnahme zu dem entspre-

chenden Eintrag vorzulegen. Ferner ist der Datenschutzbeauftragte bei der Einschätzung des Risikos nach Artikel 35 Abs. 1 der Verordnung (EU) 2016/679 oder Artikel 27 Abs. 1 der Richtlinie (EU) 2016/680 und der Prüfung, ob eine Datenschutz-Folgenabschätzung für einen konkreten Verarbeitungsvorgang durchzuführen ist, einzubeziehen.

(3) Unbeschadet von Absatz 1 hat der Datenschutzbeauftragte im Rahmen von Verarbeitungstätigkeiten im Anwendungsbereich des § 31 folgende Aufgaben:

1. Unterrichtung und Beratung der öffentlichen Stelle und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach diesem Gesetz, der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften und sonstiger Vorschriften über den Datenschutz,
2. Überwachung der Einhaltung dieses Gesetzes, der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften und sonstiger Vorschriften über den Datenschutz 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 § 52,
4. Zusammenarbeit mit dem Landesbeauftragten für den Datenschutz und
5. Tätigkeit als Anlaufstelle für den Landesbeauftragten für den Datenschutz in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation nach § 53, und gegebenenfalls Beratung zu allen sonstigen Fragen des Datenschutzes.

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

Zweiter Abschnitt

Bestimmungen für die Verarbeitung zu Zwecken nach Artikel 2 der Verordnung (EU) 2016/679

Erster Unterabschnitt

Rechtsgrundlagen der Verarbeitung

§ 16

Verarbeitung personenbezogener Daten
(Artikel 6 und 9 der Verordnung (EU) 2016/679)

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

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Abs. 1 der Verord-

nung (EU) 2016/679 ist unbeschadet anderer Rechtsvorschriften zulässig, soweit und solange

1. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit erforderlich ist,
2. sie zur Durchführung wissenschaftlicher oder historischer Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person an dem Ausschluss der Verarbeitung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann,
3. sie erforderlich ist, um den Rechten und Pflichten der öffentlichen Stellen auf dem Gebiet des Dienst- und Arbeitsrechts Rechnung zu tragen, oder
4. sie zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal, welches dem Berufsgeheimnis unterliegt, oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, erfolgt.

In den Fällen des Satzes 1 Nr. 1 bis 3 sind angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen vorzusehen.

§ 17

Zweckbindung und Zulässigkeit der Weiterverarbeitung
(Artikel 6 und 23 der Verordnung (EU) 2016/679)

(1) Als Zweck einer Verarbeitung personenbezogener Daten durch öffentliche Stellen gelten neben den ursprünglichen Zwecken immer auch die Verarbeitung

1. zur Wahrnehmung von Aufsichts- oder Kontrollbefugnissen,
2. zur Erstellung von Geschäftsstatistiken für den Verantwortlichen,
3. zur Rechnungsprüfung,
4. zur Durchführung von Organisationsuntersuchungen für den Verantwortlichen oder
5. zur Prüfung oder Wartung automatisierter Verfahren der Datenverarbeitung.

Das gilt auch für die Verarbeitung zu Ausbildungs- oder Prüfungszwecken durch den Verantwortlichen, soweit nicht offensichtlich überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen.

(2) Die Verarbeitung personenbezogener Daten zu anderen Zwecken, als zu denen sie erhoben wurden, ist vorbehaltlich spezieller Vorschriften zulässig, wenn

1. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit erforderlich ist,
2. 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 Strafgesetzbuches (StGB), von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist,
3. sie zum Schutz der Rechte und Freiheiten einer anderen Person erforderlich ist,

4. Dritte, an welche die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegen und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat,
5. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis der anderen Zwecke ihre Einwilligung verweigern würde,
6. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
7. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die Daten verarbeitende Stelle sie veröffentlichen dürfte oder
8. sie zur Sicherung des Steuer- und Zollaufkommens erforderlich ist,

sofern nicht das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Zweckänderung überwiegt. Die Verarbeitung von personenbezogenen Daten für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche und historische Forschungszwecke und statistische Zwecke ist stets zulässig. Im Übrigen hat der Verantwortliche bei der Feststellung, ob die Weiterverarbeitung mit dem Zweck der ursprünglichen Erhebung vereinbar ist, die Vorgaben des Artikels 6 Abs. 4 der Verordnung (EU) 2016/679 zu beachten. In den Fällen des Satzes 1 erfolgt eine Information der betroffenen Person nicht, soweit und solange dadurch die Zwecke der Verarbeitung gefährdet werden.

(3) Für personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage verarbeitet werden, gilt Absatz 2 nicht.

§ 18

Übermittlung

(Artikel 6 Abs. 2 der Verordnung (EU) 2016/679)

(1) Die Verantwortung für die Zulässigkeit der Übermittlung personenbezogener Daten trägt die übermittelnde Stelle. Soweit die Übermittlung aufgrund des Ersuchens eines öffentlichen Empfängers erfolgt, trägt dieser die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

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

(3) Werden personenbezogene Daten mittels eines automatisierten Verfahrens übermittelt, trägt die Verantwortung für die Zulässigkeit des einzelnen Abrufs die abrufende Stelle.

§ 19

Auftragsverarbeitung

(Artikel 28 der Verordnung (EU) 2016/679)

(1) Sind auf den Auftragsverarbeiter die Bestimmungen dieses Gesetzes, der Verordnung (EU) 2016/679 oder des Bundesdatenschutzgesetzes nicht anwendbar, ist der Verantwortliche verpflichtet, vertraglich sicherzustellen, dass der Auftragsverarbeiter die Bestimmungen der Verordnung (EU) 2016/679 und dieses Gesetzes befolgt.

(2) Der Auftrag kann auch durch die Fachaufsichtsbehörde mit Wirkung für ihrer Aufsicht unterliegenden Stellen des Landes erteilt werden; diese sind von der Auftragserteilung zu unterrichten.

**Zweiter Unterabschnitt
Rechte der betroffenen Person**

§ 20

Informationspflichten

(Artikel 13, 14 und 23 der Verordnung (EU) 2016/679)

(1) Die Informationspflichten nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679 können beschränkt werden, soweit und solange

1. die Informationen die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würden,
2. die personenbezogenen Daten oder die Tatsache ihrer Speicherung wegen einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der Rechte und Freiheiten anderer Personen, geheim gehalten werden müssen oder
3. die Information den in § 31 genannten Zwecken zuwiderlaufen würde

und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.

(2) Eine Informationspflicht besteht nicht für Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle verarbeitet werden.

(3) Werden personenbezogene Daten nicht bei der betroffenen Person, sondern bei einer nichtöffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§ 21

Auskunftsrecht

(Artikel 15 und 23 der Verordnung (EU) 2016/679)

(1) Das Auskunftsrecht nach Artikel 15 der Verordnung (EU) 2016/679 kann beschränkt werden, soweit und solange

1. die Auskunftserteilung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
2. die personenbezogenen Daten oder die Tatsache ihrer Speicherung wegen einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der Rechte und Freiheiten einer anderen Person, geheim gehalten werden müssen oder
3. die Auskunft den in § 31 genannten Zwecken zuwiderlaufen würde

und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.

(2) Das Recht auf Auskunftserteilung nach Artikel 15 der Verordnung (EU) 2016/679 gilt nicht für Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Behörden der Staatsanwaltschaften, Polizeibehörden, Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst oder, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Geschäftsbereichs des für Verteidigung zuständigen Bundesministeriums, so ist sie nur mit Zustimmung dieser Stellen zulässig. Gleiches gilt auch für den Fall der Datenübermittlung von den in Satz 1 genannten Behörden.

(4) Die Ablehnung der Auskunftserteilung bedarf keiner Begründung, soweit und solange durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf welche die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist die betroffene Person darauf hinzuweisen, dass sie sich an den Landesbeauftragten für den Datenschutz wenden kann.

(5) Wird der betroffenen Person keine Auskunft erteilt, so ist sie auf ihr Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde.

§ 22

Recht auf Einschränkung der Verarbeitung
(Artikel 18 der Verordnung (EU) 2016/679)

Als wichtiges öffentliches Interesse für eine Weiterverarbeitung der hinsichtlich ihrer Verarbeitung eingeschränkten Daten im Anwendungsbereich des Artikels 18 Abs. 2 der Verordnung (EU) 2016/679 gelten insbesondere

1. wissenschaftliche oder historische Forschungszwecke, wobei § 16 Abs. 2 Satz 1 Nr. 2 unberührt bleibt,
2. Archivzwecke,
3. Aufsichts- und Kontrollzwecke oder
4. die Rechnungsprüfung.

§ 23

Löschung personenbezogener Daten
(Artikel 17 der Verordnung (EU) 2016/679)

Soweit öffentliche Stellen verpflichtet sind, Unterlagen einem öffentlichen Archiv zur Übernahme anzubieten, ist eine Löschung erst zulässig, nachdem die Unterlagen dem öffentlichen Archiv angeboten worden sind. Das Nähere wird durch Rechtsvorschriften über öffentliche Archive geregelt.

§ 24

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
(Artikel 34 der Verordnung (EU) 2016/679)

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

1. die Information die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
2. die personenbezogenen Daten oder die Tatsache ihrer Verarbeitung nach einer Rechtsvorschrift oder wegen der Rechte und Freiheiten anderer Personen geheim zu halten sind,
3. dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten notwendig ist oder
4. die Information die Sicherheit von IT-Systemen gefährden würde.

Artikel 34 Abs. 3 der Verordnung (EU) 2016/679 bleibt davon unberührt.

Dritter Unterabschnitt Besondere Verarbeitungssituationen

§ 25

Verarbeitung personenbezogener Daten zu Zwecken der freien Meinungsäußerung und der Informationsfreiheit

(1) Soweit personenbezogene Daten in Ausübung des Rechts auf freie Meinungsäußerung und Informationsfreiheit zu journalistischen Zwecken oder zu künstlerischen oder literarischen Zwecken verarbeitet werden, gelten von den Kapiteln II bis VII sowie IX der Verordnung (EU) 2016/679 nur Artikel 5 Abs. 1 Buchst. f und die Artikel 24, 32 und 33 sowie § 83 BDSG. Artikel 82 der Verordnung (EU) 2016/679 und § 83 BDSG gelten mit der Maßgabe, dass nur für Schäden gehaftet wird, die durch eine Verletzung des Datengeheimnisses oder durch unzureichende technische oder organisatorische Maßnahmen nach Artikel 5 Abs. 1 Buchst. f und Artikel 24 der Verordnung (EU) 2016/679 eintreten.

(2) Führt die Verarbeitung personenbezogener Daten nach Absatz 1 Satz 1 zur Verbreitung von Gegendarstellungen der betroffenen Person oder zu Verpflichtungserklärungen, Beschlüssen oder Urteilen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, so sind diese Gegendarstellungen, Verpflichtungserklärungen, Beschlüsse, Urteile und Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren, wie die Daten selbst sowie bei einer Übermittlung der Daten gemeinsam zu übermitteln.

§ 26

Öffentliche Stellen, die am Wettbewerb teilnehmen

Soweit öffentliche Stellen am Wettbewerb teilnehmen, sind auf sie, auf ihre Zusammenschlüsse und Verbände von den Bestimmungen dieses Gesetzes nur die Regeln zur Aufsicht anzuwenden (§§ 3 bis 12). Im Übrigen gelten für sie die Bestimmungen des Teils 2 des Bundesdatenschutzgesetzes.

§ 27

Datenschutz im Beschäftigungskontext
(Artikel 88 der Verordnung (EU) 2016/679)

(1) Für das Verarbeiten von personenbezogenen Daten über Arbeitnehmer und Auszubildende, die in einem privatrechtlich ausgestalteten Arbeits- oder Ausbildungsver-

hältnis zu einer öffentlichen Stelle im Sinne dieses Gesetzes stehen, gelten die §§ 79 bis 87 ThürBG entsprechend, soweit besondere Rechtsvorschriften des Arbeitsrechts, tarifvertragliche Regelungen oder Dienstvereinbarungen nichts Abweichendes regeln.

(2) Erfolgt die Verarbeitung personenbezogener Daten auf der Grundlage einer Einwilligung, so bedarf diese der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die Arbeitnehmer und Auszubildenden über den Zweck der Datenverarbeitung und über ihr Widerspruchsrecht nach Artikel 7 Abs. 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

(3) Die Verarbeitung der bei medizinischen oder psychologischen Untersuchungen und Tests zum Zwecke der Eingehung eines Beschäftigungsverhältnisses im Sinne des Absatzes 1 erhobenen personenbezogenen Daten ist nur mit schriftlicher Einwilligung des Bewerbers zulässig. Der Arbeitgeber darf vom untersuchenden Arzt in der Regel nur die Übermittlung des Ergebnisses der Eignungsuntersuchung und dabei festgestellter Risikofaktoren verlangen, es sei denn, besondere Rechtsvorschriften des Arbeitsrechts oder tarifvertragliche Regelungen gehen vor.

(4) Personenbezogene Daten, die vor der Eingehung eines Beschäftigungsverhältnisses bei einer öffentlichen Stelle erhoben wurden, sind unverzüglich zu löschen, sobald feststeht, dass ein Beschäftigungsverhältnis nicht zustande kommt und die Frist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen abgelaufen ist, es sei denn, dass die betroffene Person in die weitere Speicherung eingewilligt hat.

(5) Soweit personenbezogene Daten der Arbeitnehmer und Auszubildenden einer öffentlichen Stelle im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen nach Artikel 32 der Verordnung (EU) 2016/679 gespeichert werden, dürfen sie nicht zu Zwecken der Verhaltens- und Leistungskontrolle genutzt werden.

§ 28

Verarbeitung personenbezogener Daten durch Forschungseinrichtungen (Artikel 6, 9 und 89 der Verordnung (EU) 2016/679)

(1) Für Zwecke der wissenschaftlichen oder historischen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet werden.

(2) Die Übermittlung personenbezogener Daten an Empfänger, auf die dieses Gesetz oder die Verordnung (EU) 2016/679 keine Anwendung findet, ist nur zulässig, wenn diese sich vertraglich verpflichten, die übermittelten Daten nicht für andere Zwecke zu verarbeiten und die Bestimmungen der Absätze 3 und 4 einzuhalten.

(3) Die personenbezogenen Daten sind, sobald dies nach dem Forschungszweck möglich ist, dergestalt zu verändern, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen

Person zugeordnet werden können (anonymisieren). Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(4) Die wissenschaftliche oder historische Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder soweit dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(5) Das Recht auf Auskunft, Berichtigung, Einschränkung der Verarbeitung und Widerspruch nach der Verordnung (EU) 2016/679 und diesem Gesetz besteht nicht, soweit und solange die Verwirklichung des wissenschaftlichen oder historischen Forschungsinteresses dadurch unmöglich gemacht oder erheblich beeinträchtigt wird.

§ 29

Zweckbindung von personenbezogenen Daten,
die einem Berufsgeheimnis unterliegen
(Artikel 6 und 9 der Verordnung (EU) 2016/679)

(1) Erfolgt die Datenverarbeitung durch eine öffentliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgabe, die im öffentlichen Interesse liegt, oder in Ausübung öffentlicher Gewalt, die ihr übertragen ist, dürfen die Daten, die einem Berufsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Person oder Stelle in Ausübung ihrer Berufspflicht übermittelt worden sind, von ihr nur für den Zweck verarbeitet werden, für den sie die Daten erhalten hat.

(2) Die Weiterverarbeitung für einen anderen Zweck ist zulässig, wenn die Änderung des Zwecks durch eine besondere Rechtsvorschrift nach Artikel 6 Abs. 4 in Verbindung mit Artikel 23 der Verordnung (EU) 2016/679 zugelassen ist. § 17 Abs. 2 findet keine Anwendung.

§ 30

Videoüberwachung

(1) Die Videobeobachtung oder -aufzeichnung mit Hilfe optisch-elektronischer Einrichtungen (Videoüberwachung) ist zulässig, wenn dies zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung öffentlicher Gewalt

1. zum Schutz von Personen, die der überwachenden Stelle angehören oder sie aufsuchen, oder
2. zum Schutz von Sachen, die der zu überwachenden Stelle oder den Personen nach Nummer 1 gehören, erforderlich ist. Es dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. Als besonders wichtiges öffentliches Interesse gilt der Schutz von Leben, Gesundheit oder Freiheit von Personen, die sich in der überwachenden Stelle aufhalten.

(2) Der Umstand der Videoüberwachung und die Informationen nach Artikel 13 Abs. 1 Buchst. a bis c der Verordnung (EU) 2016/679 sowie die Möglichkeit, beim Verantwortlichen die weiteren Informationen nach Artikel 13 der Verordnung (EU) 2016/679 zu erhalten, sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung der nach Absatz 1 erhobenen Daten ist zulässig, wenn dies zum Erreichen des verfolgten Zwecks erforderlich ist und unter besonderer Berücksichtigung der Belange nach Absatz 1 Satz 3 keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen.

(4) Für einen anderen Zweck dürfen nach Absatz 1 erhobene Daten nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die öffentliche Sicherheit, zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder zur Verfolgung von Straftaten erforderlich ist.

(5) Videoaufzeichnungen und aus der Videoüberwachung erhobene Daten sind abweichend von Artikel 17 Abs. 1 der Verordnung (EU) 2016/679 nicht unverzüglich zu löschen, soweit sie zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung, zur Verfolgung von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden.

Dritter Abschnitt

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

Erster Unterabschnitt

Anwendungsbereich und Grundsätze

§ 31

Anwendungsbereich

(Artikel 1 Abs. 1, Artikel 2 Abs. 1 der Richtlinie (EU) 2016/680)

Die Bestimmungen dieses Abschnitts gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche. Die Verhütung von Straftaten im Sinne des Satzes 1 umfasst den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit. Die Sätze 1 und 2 finden zudem Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 StGB, von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder von Geldbußen zuständig sind. Soweit dieser Abschnitt Bestimmungen für Auftragsverarbeiter enthält, gilt er auch für diese.

§ 32

Begriffsbestimmungen

(Artikel 3 der Richtlinie (EU) 2016/680)

Im Sinne des Dritten Abschnittes:

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, geneti-

- schen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen 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 oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder 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 Verantwortlicher die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet,
 8. ist Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet,
 9. 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 Unionsrecht oder anderen Rechtsvorschriften möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung,
 10. 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,
11. 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 natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden,
 12. sind biometrische Daten mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten,
 13. 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,
 14. 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,
 15. ist Aufsichtsbehörde eine von einem Mitgliedstaat der Europäischen Union nach Artikel 41 der Richtlinie (EU) 2016/680 eingerichtete unabhängige staatliche Stelle,
 16. ist internationale Organisation eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

§ 33

Grundsätze bei der Verarbeitung personenbezogener Daten

(Artikel 8, Artikel 4 Abs. 2 und 3, Artikel 9 Abs. 2 und 3
der Richtlinie (EU) 2016/680)

(1) Die Verarbeitung personenbezogener Daten ist zulässig, wenn diese Verarbeitung für die Aufgabenerfüllung zu den in § 31 genannten Zwecken erforderlich ist und keine spezielleren Regelungen in anderen Gesetzen vorgehen.

(2) Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen in § 31 genannten Zweck 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 § 31 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

(3) Die Verarbeitung kann zu im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder statistischen Zwecken erfolgen, wenn sie von den in § 31 genannten Zwecken umfasst ist und wenn geeignete Garantien für die Rechtsgüter der betroffenen Personen vorhanden sind. Solche Garantien können in einer frühestmöglichen Anonymisierung personenbezogener Daten, in Vorkehrungen gegen die unbefugte Kenntnisnahme durch Dritte oder in einer räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeitung personenbezogener Daten bestehen.

§ 34

Unterscheidung verschiedener Kategorien betroffener Personen sowie zwischen Tatsachen und Bewertungen (Artikel 6, Artikel 7 Abs. 1 der Richtlinie (EU) 2016/680)

(1) Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten soweit 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, oder
5. andere Personen, wie insbesondere Zeugen, Hinweisgeber oder Personen, die mit den in den Nummern 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

Satz 1 ist bei der Verfolgung und Ahndung von Ordnungswidrigkeiten und bei der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung entsprechend anzuwenden. Weitere Kategorisierungen bleiben dem jeweiligen Fachgesetz vorbehalten.

(2) Der Verantwortliche hat bei der Verarbeitung soweit 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, Beurteilungen, die auf Bewertungen oder auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. Es muss außerdem feststellbar sein, welche Stelle die Unterlagen führt, die der Bewertung oder der sonstigen auf persönlicher Einschätzung beruhenden Beurteilung zugrunde liegen.

§ 35

Berichtigung und Löschung personenbezogener Daten sowie die Einschränkung der Verarbeitung (Artikel 4 Abs. 1, Artikel 7 Abs. 3, Artikel 5 der Richtlinie (EU) 2016/680)

(1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind, und teilt der Stelle, die die personenbezogenen Daten zuvor an ihn übermittelt hat, die Berichtigung mit.

(2) Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen, wenn deren Verarbeitung unzu-

lässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder deren Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist.

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

1. Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigt würden,
2. die personenbezogenen Daten für Zwecke eines gerichtlichen Verfahrens weiter aufbewahrt werden müssen oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

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

(4) In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Absätzen 1 bis 3 hat der Verantwortliche anderen Empfängern, denen die Daten übermittelt wurden, diese Maßnahmen mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken.

(5) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen prüft der Verantwortliche regelmäßig nach festgesetzten Fristen, ob die Speicherung personenbezogener Daten für die Aufgabenerfüllung noch erforderlich ist oder die Daten zu löschen sind (Aussonderungsprüffrist). Es ist durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

§ 36

Verfahren bei Übermittlungen

(Artikel 7 Abs. 2, Artikel 9 Abs. 3 und 4 der Richtlinie (EU) 2016/680)

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

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

(3) Die übermittelnde Stelle darf auf Empfänger in anderen Mitgliedstaaten der Europäischen Union und 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.

§ 37

Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 10 der Richtlinie (EU) 2016/680)

(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 Rechtsgüter 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.

§ 38

Automatisierte Einzelentscheidung (Artikel 11 der Richtlinie (EU) 2016/680)

(1) Eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung, die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist. Die Vorschrift muss sicherstellen, dass die berechtigten Interessen und Rechtsgüter der betroffenen Person gewahrt werden. Zumindest muss sichergestellt sein, dass eine inhaltliche Bewertung und darauf gestützte Entscheidung durch den Verantwortlichen herbeigeführt und verlangt werden kann.

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

§ 39

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 wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt.

(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 sowie, wenn nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen.

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

Zweiter Unterabschnitt Rechte der betroffenen Person

§ 40

Allgemeiner Informationsanspruch
(Artikel 13 Abs. 1 der Richtlinie (EU) 2016/680)

Der Verantwortliche stellt in allgemeiner Form und für jedermann zugänglich die folgenden Informationen zur Verfügung:

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 des Datenschutzbeauftragten,
4. das Bestehen des Rechts nach § 8, den Landesbeauftragten für den Datenschutz anzurufen, und
5. die Erreichbarkeit des Landesbeauftragten für den Datenschutz.

§ 41

Benachrichtigung betroffener Personen
(Artikel 13 Abs. 2 und 3 der Richtlinie (EU) 2016/680)

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

1. die in § 40 genannten Angaben,
2. die Rechtsgrundlage der Verarbeitung,
3. die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,

4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie
5. erforderlichenfalls weitere Informationen, insbesondere wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

(2) Der Verantwortliche kann die Benachrichtigung nach Absatz 1 aufschieben, einschränken oder unterlassen, soweit und solange durch die Benachrichtigung

1. behördliche oder gerichtliche Untersuchungen, Ermittlungen oder Verfahren gefährdet werden,
 2. die Verhütung, Aufdeckung, Ermittlung oder Verfolgung von Straftaten oder die Strafvollstreckung gefährdet werden,
 3. die öffentliche Sicherheit oder Ordnung gefährdet wird oder
 4. die Rechtsgüter Dritter gefährdet werden
- und wenn das Interesse an dem Aufschub, der Einschränkung oder der Unterlassung der Benachrichtigung gegenüber dem Informationsinteresse der betroffenen Person überwiegt.

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

(4) Im Fall der Einschränkung der Benachrichtigung nach Absatz 2 gilt § 42 Abs. 6 entsprechend.

§ 42

Auskunftsrecht

(Artikel 14 bis 17 der Richtlinie (EU) 2016/680)

(1) Der Verantwortliche hat betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob er sie betreffende Daten verarbeitet. In dem Antrag sollen die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, und der Grund des Auskunftsverlangens näher bezeichnet werden. 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 personenbezogenen Daten offengelegt worden sind, insbesondere bei Empfängern in Nichtmitgliedstaaten der Europäischen Union (Drittstaaten) oder bei internationalen Organisationen,
5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer,
6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten durch den Verantwortlichen,
7. das Bestehen des Rechts nach § 8, den Landesbeauftragten für den Datenschutz anzurufen, sowie

8. die Erreichbarkeit des Landesbeauftragten für den Datenschutz.

Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst oder, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Geschäftsbereichs des für Verteidigung zuständigen Bundesministeriums, ist sie nur mit Zustimmung dieser Stellen zulässig.

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

(3) Die Auskunftserteilung unterbleibt, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand außer Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

(4) Der Verantwortliche kann unter den Voraussetzungen des § 41 Abs. 2 von der Auskunft nach Absatz 1 Satz 1 absehen oder die Auskunftserteilung nach Absatz 1 Satz 3 teilweise oder vollständig einschränken.

(5) Der Verantwortliche hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des § 41 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.

(6) Wird die betroffene Person nach Absatz 5 über die Verweigerung oder die Einschränkung der Auskunft unterrichtet, kann die betroffene Person ihr Auskunftsrecht auch über den Landesbeauftragten für den Datenschutz ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit zu unterrichten. Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen dem Landesbeauftragten für den Datenschutz zu erteilen, soweit nicht die zuständige oberste Landesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Der Landesbeauftragte für den Datenschutz hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen oder eine Überprüfung durch ihn erfolgt sind oder über die Gründe, aus denen eine Überprüfung nicht erfolgt ist. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstöße festgestellt wurden. Die Mitteilung des Landesbeauftragten für den Datenschutz an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt. Der Landesbeauftragte für

den Datenschutz hat zudem die betroffene Person über ihr Recht auf einen gerichtlichen Rechtsbehelf zu unterrichten.

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

§ 43

Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung (Artikel 16 der Richtlinie (EU) 2016/680)

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder der Beurteilung, sondern die Tatsache, dass die Aussage oder Beurteilung so erfolgt ist. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem 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 oder deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

(3) § 35 Abs. 3 und 4 gilt entsprechend.

(4) Der Verantwortliche hat die betroffene Person über eine Verweigerung der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Dies gilt nicht, wenn die Erteilung dieser Informationen eine Gefährdung im Sinne des § 41 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.

(5) § 42 Abs. 6 und 7 findet entsprechende Anwendung.

§ 44

Verfahren für die Ausübung der Rechte der betroffenen Person (Artikel 12 Abs. 1 und 3 bis 5 der Richtlinie (EU) 2016/680)

(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 grundsätzlich die für den Antrag gewählte Form verwenden.

(2) Unbeschadet des § 42 Abs. 5 und des § 43 Abs. 4 setzt der Verantwortliche die betroffene Person schriftlich darüber in Kenntnis, wie mit ihrem Antrag verfahren wurde.

(3) Informationen nach § 40, Benachrichtigungen nach § 41, Mitteilungen nach § 56 und die Bearbeitung von Anträgen nach den §§ 42 und 43 erfolgen für die betroffene Person unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen der betroffenen Person nach den §§ 42 und 43 kann der Verantwortliche entweder Verwaltungskosten auf der Grundlage des Verwaltungsaufwands verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall trägt der Verantwortliche die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter des Antrags.

(4) Hat der Verantwortliche begründete Zweifel an der Identität der betroffenen Person, die den Antrag nach den §§ 42 oder 43 stellt, so kann er bei der betroffenen Person zusätzliche Informationen oder Nachweise anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

§ 45

Schadensersatz

(Artikel 56 der Richtlinie (EU) 2016/680)

(1) Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder nach anderen auf deren 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 nichtautomatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.

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

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

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

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

Dritter Unterabschnitt Pflichten der Verantwortlichen und Auftragsverarbeiter

§ 46

Pflichten des Verantwortlichen

(Artikel 20 der Richtlinie (EU) 2016/680)

(1) Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene Vorkehrungen zu treffen, die geeignet sind, Datenschutzgrundsätze wie etwa Datensparsamkeit wirksam umzusetzen und die notwendigen 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 Gefährdung für die Rechtsgüter der betroffenen Personen zu berücksichtigen.

(2) Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang deren Verarbeitung, deren Speicherdauer und deren Zugänglichkeit. Die Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

§ 47

Gemeinsam Verantwortliche (Artikel 21 der Richtlinie (EU) 2016/680)

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

§ 48

Auftragsverarbeitung (Artikel 22 der Richtlinie (EU) 2016/680)

(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 Person 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 Absatz 6 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 Einhaltung genehmigter Verhaltensregeln nach Artikel 40 der Verordnung (EU) 2016/679 oder eines genehmigten Zertifizierungsverfahrens nach Artikel 42 der Verordnung (EU) 2016/679 durch einen Auftragsverarbeiter kann als Faktor herangezogen werden, um hinreichende Garantien im Sinne der Absätze 2 und 4 nachzuweisen.

(6) 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 personenbezogenen Daten besteht,
5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die nach § 51 generierten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt,
6. Überprüfungen, die von dem Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt,
7. die in den Absätzen 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält,
8. alle nach § 54 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 §§ 52 bis 56 genannten Pflichten unterstützt.

(7) Der Vertrag oder ein anderes Rechtsinstrument im Sinne des Absatzes 6 sind schriftlich oder elektronisch abzufassen.

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

§ 49

Verarbeitung auf Weisung, Datengeheimnis (Artikel 23 der Richtlinie (EU) 2016/680)

(1) Jede einem Verantwortlichen oder einem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese nicht unbefugt verarbeiten (Datengeheimnis), sondern ausschließlich auf Weisung des Verantwortlichen, es sei denn, dass sie nach einer Rechtsvorschrift zur Verarbeitung verpflichtet ist.

(2) Die mit der Datenverarbeitung befassten Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.

§ 50

Verzeichnis von Verarbeitungstätigkeiten (Artikel 24 der Richtlinie (EU) 2016/680)

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

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten 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,
4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
5. gegebenenfalls die Verwendung von Profiling,
6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation,
7. Angaben über die Rechtsgrundlage der Verarbeitung,
8. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und
9. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 54.

(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 des Datenschutzbeauftragten,
2. gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation, sofern dies von dem Verantwortlichen entsprechend angewiesen wird, einschließlich der Identifizierung des Drittstaats oder der internationalen Organisation und
3. eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen nach § 54.

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

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

§ 51

Protokollierung

(Artikel 25 der Richtlinie (EU) 2016/680)

(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 soweit 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 für die Überprüfung der Rechtmäßigkeit der Datenverarbeitung durch den Datenschutzbeauftragten, den Landesbeauftragten für den Datenschutz und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.

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

(5) Der Verantwortliche und der Auftragsverarbeiter stellen die Protokolle dem Landesbeauftragten für den Datenschutz auf Anforderung zur Verfügung.

§ 52

Durchführung einer Datenschutz-Folgenabschätzung

(Artikel 27 der Richtlinie (EU) 2016/680)

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine hohe Gefährdung für die Rechtsgü-

ter betroffener Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen.

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

(3) Der Verantwortliche beteiligt den Datenschutzbeauftragten an der Durchführung der Datenschutz-Folgenabschätzung.

(4) Die Datenschutz-Folgenabschätzung hat den Rechten der von der Verarbeitung betroffenen Personen 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 den Zweck,
3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und
4. die Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, einschließlich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden soll.

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

§ 53

Anhörung des Landesbeauftragten für den Datenschutz
(Artikel 28 der Richtlinie (EU) 2016/680)

(1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen den Landesbeauftragten für den Datenschutz anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach § 52 hervorgeht, dass die Verarbeitung eine hohe Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hätte, wenn der Verantwortliche keine Abhilfemaßnahmen treffen würde, oder
2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hat.

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

(2) Dem Landesbeauftragten für den Datenschutz sind im Fall des Absatzes 1 vorzulegen:

1. die nach § 52 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 den Mitteln der beabsichtigten Verarbeitung,
4. Angaben zu den zum Schutz der Rechtsgüter der betroffenen Personen vorgesehenen Maßnahmen und Garantien und
5. der Name und die Kontaktdaten des Datenschutzbeauftragten.

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

(3) Falls der Landesbeauftragte für den Datenschutz der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstoßen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemaßnahmen getroffen hat, kann er dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Maßnahmen noch ergriffen werden sollten. Der Landesbeauftragte für den Datenschutz kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. Er hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung 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 vor Eingang der schriftlichen Empfehlungen des Landesbeauftragten für den Datenschutz beginnen. In diesem Fall sind die Empfehlungen des Landesbeauftragten für den Datenschutz im Nachhinein zu berücksichtigen und die Art und Weise der Verarbeitung gegebenenfalls anzupassen.

Vierter Unterabschnitt Datensicherheit

§ 54

Anforderungen an die Sicherheit der Datenverarbeitung
(Artikel 29 der Richtlinie (EU) 2016/680)

(1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mit-

tel in Anbetracht der Verarbeitungszwecke möglich sind. Die Maßnahmen nach Absatz 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall umgehend wiederhergestellt werden können.

(3) Bei der automatisierten Verarbeitung ergreift der Verantwortliche oder der Auftragsverarbeiter nach einer Risikobewertung Maßnahmen, die Folgendes bezwecken:

1. Verwehrung des Zugangs durch Unbefugte zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird (Zugangskontrolle),
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle),
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle),
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben (Zugriffskontrolle),
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle),
8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird (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) und
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.

§ 55

Meldung von Verletzungen des Schutzes
personenbezogener Daten an den
Landesbeauftragten für den Datenschutz
(Artikel 30 der Richtlinie (EU) 2016/680)

(1) Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem ihm diese bekannt wurden, dem Landesbeauftragten für den Datenschutz zu melden, es sei denn, dass die Verletzung voraussichtlich keine Gefahr für die Rechtsgüter natürlicher Personen darstellt. Erfolgt die Meldung an den Landesbeauftragten für den Datenschutz nicht innerhalb von 72 Stunden, ist der Meldung eine Begründung für die Verzögerung beizufügen.

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

(3) Die Meldung nach Absatz 1 enthält zumindest folgende Informationen:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen, der betroffenen Kategorien personenbezogener Daten und der ungefähren Anzahl der betroffenen personenbezogenen Datensätze,
2. Name und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann,
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 der getroffenen Maßnahmen zur Abmilderung seiner möglichen nachteiligen Auswirkungen.

(4) Wenn die Informationen nicht zur gleichen Zeit bereitgestellt werden können, hat der Verantwortliche diese Informationen unverzüglich schrittweise zur Verfügung zu stellen.

(5) Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten nach Absatz 1 einschließlich aller im Zusammenhang mit ihnen stehenden Tatsachen, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen zu dokumentieren.

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

(7) Weitere Pflichten des Verantwortlichen zur Benachrichtigung über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

§ 56

Benachrichtigung der betroffenen Person bei Verletzungen des Schutzes personenbezogener Daten (Artikel 31 der Richtlinie (EU) 2016/680)

(1) Wenn eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine hohe Gefährdung für die Rechtsgüter natürlicher Personen zur Folge hat, so hat der Verantwortliche die betroffenen Personen unverzüglich von der Verletzung zu benachrichtigen.

(2) Die Benachrichtigung der betroffenen Personen nach Absatz 1 beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in § 55 Abs. 3 Nr. 2 bis 4 genannten Informationen und Maßnahmen.

(3) Die Benachrichtigung der betroffenen Personen nach Absatz 1 ist nicht erforderlich, wenn

1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen auf die von der Verletzung des Schutzes betroffenen personenbezogenen Daten angewandt hat, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung,
2. der Verantwortliche durch im Anschluss an die Verletzung getroffene Maßnahmen sichergestellt hat, dass die erhebliche Gefahr für die Rechtsgüter der betroffenen Personen nach Absatz 1 aller Wahrscheinlichkeit nach 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 nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann der Landesbeauftragte für den Datenschutz unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einer erheblichen Gefahr führt, von dem Verantwortlichen verlangen, dies nachzuholen oder förmlich feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind.

(5) Die Benachrichtigung der betroffenen Personen nach Absatz 1 kann unter den in § 41 Abs. 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden.

Fünfter Unterabschnitt
Übermittlung personenbezogener Daten an
Drittstaaten oder internationale Organisationen

§ 57

Allgemeine Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten und internationale Organisationen (Artikel 35 und 36 der Richtlinie (EU) 2016/680)

(1) Die Übermittlung personenbezogener Daten an Stellen in einem Drittstaat oder internationale Organisationen, die

für die in § 31 genannten Zwecke zuständig sind, ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn die Europäische Kommission nach Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat.

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

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

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

§ 58

Datenübermittlung bei geeigneten Garantien
(Artikel 37 der Richtlinie (EU) 2016/680)

(1) Liegt kein Beschluss nach Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 57 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 zum Schutz personenbezogener Daten bestehen.

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

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

§ 59

Datenübermittlung ohne Angemessenheitsbeschluss und ohne geeignete Garantien (Artikel 38 der Richtlinie (EU) 2016/680)

(1) Liegen weder ein Beschluss nach Artikel 36 Abs. 3 der Richtlinie (EU) 2016/680 noch geeignete Garantien nach § 58 Abs. 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des § 57 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 § 31 genannten Zwecke oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in § 31 genannten Zwecken.

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

(3) § 58 Abs. 2 und 3 gilt entsprechend.

§ 60

Sonstige Datenübermittlung an Empfänger in Drittstaaten (Artikel 39 der Richtlinie (EU) 2016/680)

(1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall personenbezogene Daten direkt an Stellen in Drittstaaten, die nicht für die in § 31 genannten Zwecke zuständig sind, übermitteln, wenn die Übermittlung für die Aufgabenerfüllung 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 für die in § 31 genannten Zwecke zuständige Stelle wirkungslos oder ungeeignet ist,

insbesondere weil die Übermittlung nicht rechtzeitig durchgeführt werden kann, und

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

(2) Der Verantwortliche hat die für die in § 31 genannten Zwecke zuständige Stelle, an die abweichend von § 57 nicht übermittelt wurde, unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

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

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

(5) § 58 Abs. 2 und 3 gilt entsprechend.

Vierter Abschnitt Ordnungswidrigkeiten und Strafbestimmungen

§ 61

Ordnungswidrigkeiten und Strafbestimmungen

(1) Ordnungswidrig handelt, wer entgegen den Bestimmungen der Verordnung (EU) 2016/679, dieses Gesetzes oder einer anderen Rechtsvorschrift über den Schutz personenbezogener Daten solche Daten

1. erhebt, speichert, verändert, übermittelt oder nutzt,
2. zum Abruf mittels automatisierten Verfahrens bereithält,
3. abrufen oder sich oder einem anderen aus Dateien verschafft oder
4. sonst verarbeitet.

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

(3) Ebenso kann mit Geldbuße bis zu fünfzigtausend Euro belegt werden, wer die Übermittlung von personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht.

(4) Gegen öffentliche Stellen nach § 2 Abs. 1 und 2 werden keine Geldbußen verhängt, es sei denn, es handelt sich um öffentliche Stellen, die am Wettbewerb im Sinne des § 26 teilnehmen.

(5) Wer bei einer Handlung nach den Absätzen 1 und 3 gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person und der Landesbeauftragte für den Datenschutz.

(6) Der Landesbeauftragte für den Datenschutz ist Verwaltungsbehörde im Sinne des § 36 Abs. 1 Nr. 1 des Gesetzes über Ordnungswidrigkeiten in der Fassung vom 19. Februar 1987 (BGBl. I S. 602) in der jeweils geltenden Fassung.

Fünfter Abschnitt **Orden und Ehrenzeichen, Gnadensachen**

§ 62 Orden und Ehrenzeichen

Sofern personenbezogene Daten zur Entscheidung über die Verleihung von staatlichen Orden oder Ehrenzeichen verarbeitet werden, ist der Verantwortliche nicht zur Informations- und Auskunftserteilung nach den Artikeln 13 bis 15 der Verordnung (EU) 2016/679 sowie den §§ 20 und 21 verpflichtet.

§ 63 Gnadensachen

§ 62 gilt entsprechend für die Datenverarbeitung in Gnadensachen.

Sechster Abschnitt **Übergangs- und Schlussbestimmungen**

§ 64 Übergangsbestimmungen

(1) Die Amtszeit des Landesbeauftragten für den Datenschutz, der am 24. Mai 2018 das Amt des Landesbeauftragten für den Datenschutz innehat, wird durch das Inkrafttreten dieses Gesetzes nicht unterbrochen. Hat der Landesbeauftragte für den Datenschutz das Amt am 24. Mai 2018 bereits aufgrund einer Wiederwahl inne, ist eine nochmalige Wiederwahl nicht möglich. § 5 Abs. 3 Satz 2 gilt nicht für den Amtsinhaber nach Satz 1.

(2) Der Landesbeauftragte für den Datenschutz, welcher zum Zeitpunkt des Inkrafttretens dieses Gesetzes bestellt ist, gilt als Aufsichtsbehörde im Sinne dieses Gesetzes.

(3) In dem Jahresbericht für das Jahr 2018 nach § 10 Abs. 1 und § 11 Abs. 2 ist für den Berichtszeitraum vom 1. Januar 2018 bis zum 24. Mai 2018 das Thüringer Datenschutzgesetz in der am 24. Mai 2018 geltenden Fassung zugrunde zu legen.

(4) Die am 25. Mai 2018 im Anwendungsbereich des Dritten Abschnitts eingerichteten automatisierten Verarbeitungssysteme sind zeitnah, in Ausnahmefällen, in denen die Anpassung mit einem unverhältnismäßigem Aufwand verbunden ist, jedoch spätestens bis zum 6. Mai 2023, mit § 51 in Einklang zu bringen.

§ 65 Gleichstellungsbestimmung

Status- und Funktionsbezeichnungen in diesem Gesetz gelten jeweils in männlicher und weiblicher Form.

Artikel 2
Änderung des Thüringer Gesetzes über das
Verfahren bei Bürgerantrag, Volksbegehren und
Volksentscheid

Das Thüringer Gesetz über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid in der Fassung vom 23. Februar 2004 (GVBl. S. 237) wird wie folgt geändert:

1. § 5 wird wie folgt geändert:
 - a) In Absatz 1 Satz 1 werden die Worte "und genutzt" gestrichen.
 - b) In Absatz 2 werden die Worte "oder nutzt" gestrichen.
2. In § 6 Abs. 1 Satz 3 werden die Worte "und genutzt" gestrichen.

Artikel 3
Änderung des Ordnungsbehördengesetzes

Das Ordnungsbehördengesetz vom 18. Juni 1993 (GVBl. S. 323), zuletzt geändert durch Artikel 2 des Gesetzes vom 19. September 2013 (GVBl. S. 251), wird wie folgt geändert:

1. § 26 erhält folgende Fassung:

"§ 26
Datenschutz

(1) Sofern Ordnungsbehörden Daten im Rahmen der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung verarbeiten, finden der Erste, Dritte und Vierte Abschnitt des Thüringer Datenschutzgesetzes (ThürDSG) Anwendung; im Übrigen gilt die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) in Verbindung mit dem Ersten, Zweiten, Vierten und Sechsten Abschnitt des Thüringer Datenschutzgesetzes, mit der Maßgabe der Absätze 2 bis 5.

(2) Die Ordnungsbehörden können personenbezogene Daten, auch durch Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen, bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen, oder zur Erfüllung ihrer sonstigen Aufgaben nur erheben, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Gefahren für die öffentliche Sicherheit oder Ordnung entstehen. Die Unterlagen sind spätestens zwei Monate nach Ablauf des auslösenden Ereignisses zu vernichten, soweit sie nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden.

(3) Für Datenerhebungen bei oder im Zusammenhang mit öffentlichen Versammlungen und Aufzügen gelten die §§ 12a und 19a des Versammlungsgesetzes.

(4) Stellen die Ordnungsbehörden fest, dass bei der Verarbeitung von Daten im Rahmen der Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung unrichtige oder unzulässig gespeicherte personenbezogene Daten übermittelt worden sind und ist der Empfänger bekannt, gelten die §§ 35 und 43 ThürDSG.

(5) In Ausführung von § 35 Abs. 5 ThürDSG findet § 40 Abs. 4 und 5 PAG entsprechend Anwendung."

2. Die Inhaltsübersicht wird den vorstehenden Änderungen angepasst.

Artikel 4 Änderung des Polizeiaufgabengesetzes

Das Polizeiaufgabengesetz vom 4. Juni 1992 (GVBl. S. 199), zuletzt geändert durch Artikel 6 des Gesetzes vom 8. August 2014 (GVBl. S. 529), wird wie folgt geändert:

1. In § 12 Abs. 1 wird die Verweisung "§§ 13 bis 47" durch die Verweisung "§§ 13 bis 44" ersetzt.
2. In § 25 Abs. 2 wird der Klammerzusatz "(§ 104 Abs. 3 der Strafprozeßordnung)" durch den Klammerzusatz "(§ 104 Abs. 3 StPO)" ersetzt.
3. § 31 erhält folgende Fassung:

"§ 31 Anwendbares Recht

Die Polizei kann personenbezogene Daten zur Erfüllung der polizeilichen Aufgaben im Sinne des § 2 zur Abwehr von Gefahren für die öffentliche Sicherheit und zur Verhütung von Straftaten sowie zum Zwecke der Verhütung und Verfolgung von Straftaten verarbeiten, soweit dies durch dieses Gesetz in Verbindung mit den Bestimmungen des Ersten und Dritten Abschnitts des Thüringer Datenschutzgesetzes (ThürDSG) oder besonderer Rechtsvorschriften über die Datenerhebung der Polizei zugelassen ist."

4. § 32 wird wie folgt geändert:
 - a) Die Überschrift erhält folgende Fassung:

"Grundsätze der Datenerhebung"
 - b) In Absatz 1 wird die Verweisung "§§ 12 bis 47" durch die Verweisung "§§ 12 bis 44" ersetzt.
 - c) Folgende Absätze 3 bis 5 werden angefügt:

"(3) Personenbezogene Daten sind grundsätzlich bei den betroffenen Personen zu erheben. Personenbezogene Daten der betroffenen Person können auch bei Behörden, öffentlichen Stellen oder bei Dritten erhoben werden, wenn die Datenerhebung bei der betroffenen Person nicht oder nur

mit unverhältnismäßig hohem Aufwand möglich ist oder die Erfüllung der polizeilichen Aufgaben gefährden würde.

(4) Personenbezogene Daten sind von der Polizei grundsätzlich offen zu erheben. Eine Datenerhebung, die nicht als polizeiliche Maßnahme erkennbar ist oder sein soll, ist zulässig, wenn die Erfüllung polizeilicher Aufgaben auf andere Weise gefährdet oder erheblich erschwert würde oder wenn anzunehmen ist, dass dies den überwiegenden Interessen der betroffenen Person entspricht.

(5) Werden Daten bei der betroffenen Person oder bei Dritten offen erhoben, sind diese in geeigneter Weise auf

1. die Rechtsgrundlage der Datenerhebung und
2. eine im Einzelfall bestehende gesetzliche Auskunftspflicht oder die Freiwilligkeit der Auskunft hinzuweisen. Der Hinweis kann zunächst unterbleiben, wenn hierdurch die Erfüllung der polizeilichen Aufgabe oder die schutzwürdigen Belange Dritter beeinträchtigt oder gefährdet würden."

5. § 34 Abs. 4 Satz 4 erhält folgende Fassung:

"Tritt die Anordnung nach Satz 3 außer Kraft, sind die erhobenen Daten unverzüglich zu löschen und die Löschung zu protokollieren."

6. Dem § 34 a Abs. 5 wird folgender Satz angefügt:

"Tritt die Anordnung nach Satz 3 außer Kraft, sind die erhobenen Daten unverzüglich zu löschen und die Löschung zu protokollieren."

7. § 36 Abs. 3 Satz 1 Nr. 9 wird wie folgt geändert:

- a) In Buchstabe b wird das Komma durch einen Punkt ersetzt.
- b) Buchstabe c wird aufgehoben.

8. Die §§ 38 und 39 werden aufgehoben.

9. Die §§ 40 und 41 erhalten folgende Fassung:

"§ 40
Weiterverarbeitung von Daten

(1) Die Polizei kann rechtmäßig erlangte personenbezogene Daten weiterverarbeiten, soweit dies zur Erfüllung ihrer Aufgaben, zu einer zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung erforderlich ist.

(2) Dabei kann die Polizei auch die im Rahmen der Verfolgung von Straftaten gewonnenen personenbezogenen Daten zum Zwecke der Gefahrenabwehr nach § 2 Abs. 1 weiterverarbeiten von

1. Verurteilten,
2. Beschuldigten,
3. Personen, die einer Straftat verdächtig sind, sofern die Weiterverarbeitung der Daten erforderlich ist, weil wegen der Art oder Ausführung der Tat, der

Persönlichkeit der betroffenen Person oder sonstiger Erkenntnisse Grund zu der Annahme besteht, dass zukünftig Strafverfahren gegen sie zu führen sind, oder

4. Personen, bei denen Anlass zur Weiterverarbeitung der Daten besteht, weil tatsächliche Anhaltspunkte dafür vorliegen, dass die betroffenen Personen in naher Zukunft Straftaten von erheblicher Bedeutung begehen werden (Anlasspersonen).

(3) Soweit dies zur Verhütung oder zur Vorsorge für die künftige Verfolgung einer Straftat mit erheblicher Bedeutung erforderlich ist, kann die Polizei personenbezogene Daten von Personen weiterverarbeiten, bei denen tatsächliche Anhaltspunkte dafür vorliegen, dass

1. sie bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen,
2. sie als Opfer einer künftigen Straftat in Betracht kommen,
3. sie mit in Absatz 2 Nr. 1 bis 3 bezeichneten Personen nicht nur flüchtig oder in zufälligem Kontakt und in einer Weise in Verbindung stehen, die erwarten lässt, dass Hinweise für die Verfolgung oder vorbeugende Bekämpfung dieser Straftaten gewonnen werden können, weil Tatsachen die Annahme rechtfertigen, dass die Personen von der Planung oder der Vorbereitung der Straftaten oder der Verwertung der Tatvorteile Kenntnis haben oder daran mitwirken, oder
4. es sich um Hinweisgeber und sonstige Auskunftspersonen handelt.

Personenbezogene Daten über Personen nach Satz 1 Nr. 1, 2 oder 4 dürfen nur mit Einwilligung der betroffenen Person gespeichert werden. Die Einwilligung ist nicht erforderlich, wenn das Bekanntwerden der Speicherungsabsicht den mit der Speicherung verfolgten Zweck gefährden würde.

(4) Die Polizei kann personenbezogene Daten zur polizeilichen Aus- und Fortbildung nutzen. Die personenbezogenen Daten sind zu anonymisieren. Einer Anonymisierung bedarf es nicht, wenn diese dem Aus- und Fortbildungszweck entgegensteht und die berechtigten Interessen der betroffenen Person an der Geheimhaltung der Daten nicht offensichtlich überwiegen.

(5) Die Dauer der Speicherung ist auf das erforderliche Maß zu beschränken. Es sind Fristen festzulegen, zu denen spätestens zu prüfen ist, ob die Speicherung personenbezogener Daten für die Aufgabenerfüllung noch erforderlich ist (Aussonderungsprüffristen). Die Aussonderungsprüffristen dürfen bei Verarbeitungen nach Absatz 2 bei Erwachsenen zehn Jahre, bei Jugendlichen fünf Jahre und bei Kindern zwei Jahre nicht überschreiten, wobei nach Zweck der Speicherung sowie Art und Schwere des Sachverhalts zu unterscheiden ist. In den Fällen des Absatzes 3 dürfen die Aussonderungsprüffristen bei Erwachsenen fünf Jahre und bei Jugendlichen drei Jahre nicht überschreiten. Personenbezogene Daten der in Absatz 3 bezeichneten Personen können ohne Zustimmung der betroffenen Person nur für die Dauer eines Jahres gespeichert werden. Die Speicherung für jeweils ein weiteres Jahr ist zulässig, soweit die Voraussetzungen des Absatzes 3

weiterhin vorliegen. Die maßgeblichen Gründe für die Aufrechterhaltung der Speicherung nach Satz 4 sind aktenkundig zu machen.

(6) Die Fristen nach Absatz 5 Satz 2 bis 6 beginnen für alle zu einer Person gespeicherten Daten mit dem Tag, an dem die betroffene Person letztmalig zur Speicherung nach diesem Gesetz Anlass gegeben hat, jedoch nicht vor Entlassung der betroffenen Person aus einer Justizvollzugsanstalt oder Beendigung einer mit Freiheitsentziehung verbundenen Maßregel der Besserung und Sicherung. Die Speicherung kann über die in Absatz 5 Satz 3 genannten Fristen hinaus auch allein für Zwecke der Vorgangsverwaltung aufrechterhalten werden, sofern dies erforderlich ist; in diesem Fall können die Daten nur noch für diesen Zweck oder zur Behebung einer bestehenden Beweisnot verwendet werden. Wird ein Beschuldigter rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, so ist die Weiterverarbeitung unzulässig, wenn sich aus den Gründen der Entscheidung ergibt, dass die betroffene Person die Tat nicht oder nicht rechtswidrig begangen hat.

(7) Das für die Polizei zuständige Ministerium wird ermächtigt, durch Rechtsverordnung weitere Kriterien für die Festlegung der Aussonderungsprüffristen zu regeln.

§ 41

Datenübermittlung im innerstaatlichen Bereich

(1) Die Polizei kann personenbezogene Daten an Dienststellen der Polizei oder andere für die Gefahrenabwehr zuständige Behörden oder öffentliche Stellen übermitteln, soweit dies zur Erfüllung polizeilicher Aufgaben oder zur Erfüllung der Aufgaben des Empfängers erforderlich ist. Die Übermittlung personenbezogener Daten an das Amt für Verfassungsschutz richtet sich nach dem Thüringer Verfassungsschutzgesetz.

(2) An andere Behörden, öffentliche oder nicht öffentliche Stellen sowie Einzelpersonen kann die Polizei personenbezogene Daten übermitteln, soweit dies

1. in anderen Rechtsvorschriften vorgesehen ist oder
2. zulässig oder erforderlich ist zur
 - a) Erfüllung polizeilicher Aufgaben,
 - b) Abwehr einer Gefahr durch den Empfänger oder
 - c) Verhütung oder Beseitigung erheblicher Nachteile für das Gemeinwohl oder für die schutzwürdigen Belange Einzelner.

(3) Andere Behörden und sonstige öffentliche Stellen können personenbezogene Daten an die Polizei übermitteln, soweit dies zur Erfüllung polizeilicher Aufgaben erforderlich ist. Auf Verlangen sind die Daten zu übermitteln. Die Polizei darf entsprechende Übermittlungsersuchen nur stellen, wenn die Voraussetzungen für die Datenerhebung vorliegen. Andere besondere Rechtsvorschriften über die Datenübermittlung bleiben unberührt.

(4) Die Polizei kann personenbezogene Daten nach Absatz 2 nur zu dem Zweck übermitteln, zu dem sie die Daten erhoben oder gespeichert hat. Abweichend hiervon kann die Polizei nach Maßgabe des Absatzes 2 personenbezogene Daten übermitteln, soweit dies für die Erfüllung dort genannter Aufgaben durch den Empfänger unerlässlich ist und dieser die Daten auf andere Weise nicht oder nicht rechtzeitig oder nur mit unverhältnismäßig hohem Aufwand erlangen kann. Bei der Übermittlung von personenbezogenen Daten teilt die Polizei dem Empfänger die bestehenden Lösungsverpflichtungen mit.

(5) Unterliegen die von der Polizei zu übermittelnden Daten einem Berufs- oder besonderen Amtsgeheimnis, ist für die Zulässigkeit der Übermittlung durch die Polizei ferner erforderlich, dass der Empfänger die Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie die Polizei erhoben hat oder hätte erheben können.

(6) Die übermittelnde Dienststelle der Polizei prüft die Zulässigkeit der Übermittlung. Erfolgt die Übermittlung aufgrund eines Ersuchens einer anderen öffentlichen Stelle, hat die übermittelnde Stelle lediglich zu prüfen, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Empfängers liegt. Die Zulässigkeit der Übermittlung im Übrigen prüft sie nur, wenn hierfür im Einzelfall besonderer Anlass besteht. Der Empfänger hat der übermittelnden Stelle die zur Prüfung erforderlichen Angaben zu machen.

(7) Der Empfänger darf die übermittelten personenbezogenen Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck nutzen, zu dem sie ihm übermittelt worden sind."

10. Die §§ 41 b bis 41 d erhalten folgende Fassung:

"§ 41 b
Datenübermittlung an Mitgliedstaaten der
Europäischen Union

(1) § 41 gilt entsprechend für die Übermittlung von personenbezogenen Daten an

1. öffentliche und nichtöffentliche Stellen in Mitgliedstaaten der Europäischen Union und
2. zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben der Verhütung und Verfolgung von Straftaten befasst sind.

(2) Für die Übermittlung an Polizei- und Justizbehörden sowie an sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stellen zum Zwecke der Verfolgung von Straftaten und zur Strafvollstreckung bleiben die Vorschriften über die internationale Rechtshilfe in strafrechtlichen Angelegenheiten unberührt. Die Zulässigkeit der Übermittlung personenbezogener Daten an eine Polizeibehörde oder eine sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union auf der Grundlage besonderer völkerrechtlicher Vereinbarungen bleibt unberührt.

(3) Die Absätze 1 und 2 finden auch Anwendung auf die Übermittlung von personenbezogenen Daten an Polizeibehörden oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stellen von Staaten, welche die Bestimmungen des Schengen-Besitzstandes aufgrund eines Assoziierungsabkommens mit der Europäischen Union über die Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstandes anwenden.

(4) Die Bestimmungen des Beschlusses 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 1) sind bei der polizeilichen Zusammenarbeit mit den Mitgliedstaaten der Europäischen Union anwendbar.

§ 41 c

Datenübermittlung im internationalen Bereich

Die Polizei kann bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen personenbezogene Daten an Polizei- und Justizbehörden sowie an sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stellen in anderen als den in § 41 b Abs. 1 genannten Staaten (Drittstaaten) und an andere als die in § 41 b Abs. 1 genannten zwischen- und überstaatlichen Stellen, die mit Aufgaben der Verhütung oder Verfolgung von Straftaten befasst sind, übermitteln, soweit dies erforderlich ist

1. zur Erfüllung einer ihr obliegenden Aufgabe,
2. zur Verfolgung von Straftaten und zur Strafverfolgung nach Maßgabe der Vorschriften über die internationale Rechtshilfe in strafrechtlichen Angelegenheiten oder der Vorschriften über die Zusammenarbeit mit dem Internationalen Strafgerichtshof oder
3. zur Abwehr einer im Einzelfall bestehenden erheblichen Gefahr für die öffentliche Sicherheit.

Entsprechendes gilt, wenn Anhaltspunkte dafür vorliegen, dass Straftaten von erheblicher Bedeutung begangen werden sollen. Die übermittelnde Stelle hat die Übermittlung und ihren Anlass aufzuzeichnen und dem Empfänger den bei der übermittelnden Stelle vorgesehenen Lösungszeitpunkt mitzuteilen.

§ 41 d

Übermittlungsverbote

(1) Die Übermittlung nach den Vorschriften dieses Gesetzes unterbleibt, wenn für die übermittelnde Stelle erkennbar ist, dass unter Berücksichtigung der Art der Daten und ihrer Erhebung die schutzwürdigen Interessen der betroffenen Person das Allgemeininteresse an der Übermittlung überwiegen.

(2) Die Datenübermittlung nach den §§ 41 b und 41 c unterbleibt darüber hinaus,

1. wenn hierdurch wesentliche Sicherheitsinteressen des Bundes oder der Länder beeinträchtigt würden,
2. wenn hierdurch der Erfolg laufender Ermittlungen oder Leib, Leben oder Freiheit einer Person gefährdet würde,

3. soweit Grund zu der Annahme besteht, dass durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde, oder
 4. wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die Übermittlung der Daten zu den in der Charta der Grundrechte der Europäischen Union enthaltenen Grundsätzen, insbesondere dadurch, dass durch die Nutzung der übermittelten Daten im Empfängerstaat Verletzungen von elementaren rechtsstaatlichen Grundsätzen oder Menschenrechtsverletzungen drohen, in Widerspruch stünde."
11. § 42 Abs. 2 Satz 2 wird aufgehoben.
12. § 43 Abs. 1 wird wie folgt geändert:
- a) In Satz 2 werden die Worte "geboten erscheint" durch die Worte "erforderlich ist" ersetzt.
 - b) In Satz 3 werden nach dem Wort "abgleichen" ein Komma und die Worte "wenn dies zur Erfüllung polizeilicher Aufgaben erforderlich ist" angefügt.
13. Die §§ 45 bis 47 werden aufgehoben.
14. In § 54 Abs. 4 Satz 2 wird die Angabe "7. August 1991 (GVBl. S. 321)" durch die Angabe "23. September 2005 (GVBl. S. 325)" ersetzt.
15. Die Inhaltsübersicht wird den vorstehenden Änderungen angepasst.

Artikel 5

Änderung des Thüringer Kommunalwahlgesetzes

Das Thüringer Kommunalwahlgesetz vom 16. August 1993 (GVBl. S. 530), zuletzt geändert durch Artikel 2 des Gesetzes vom 24. April 2017 (GVBl. S. 89), wird wie folgt geändert:

1. § 5 wird wie folgt geändert:
 - a) Absatz 4 wird wie folgt geändert:
 - aa) In Satz 1 werden die Worte "zu erheben," und die Worte "und zu nutzen" gestrichen.
 - bb) Die Sätze 2 und 3 erhalten folgende Fassung:

"Zu diesem Zweck dürfen personenbezogene Daten von Wahlberechtigten, die zur Tätigkeit in Wahlvorständen geeignet sind, bis zum Ablauf der Wahlperiode verarbeitet werden. Soweit der Wahlberechtigte seine Einwilligung erteilt, dürfen die personenbezogenen Daten auch für zukünftige Wahlen verarbeitet werden."
 - cc) In Satz 4 werden das Wort "erhoben," und die Worte "und genutzt" gestrichen.

b) Absatz 5 erhält folgende Fassung:

"(5) Auf Ersuchen der Gemeinde sind zur Sicherstellung der Durchführung der Wahl Behörden des Landes, der Gemeinden, der Landkreise und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts berechtigt, aus dem Kreis ihrer Bediensteten unter Angabe von Name, Vorname, Geburtsdatum und Anschrift zum Zweck der Berufung zu Mitgliedern der Wahlvorstände Personen, die im Gebiet der ersuchenden Gemeinde wohnen, zu benennen, wenn der Bedienstete in die Datenübermittlung eingewilligt hat. Für die Mitwirkung im Wahlvorstand ist der Bedienstete freizustellen."

2. § 36 erhält folgende Fassung:

"§ 36
Wahlstatistik, Information der Öffentlichkeit

(1) Die Ergebnisse der Gemeindewahlen und der Landkreiswahlen sind vom Landesamt für Statistik statistisch zu bearbeiten. Die Gemeinden und die Landkreise übermitteln dem Landesamt die dafür erforderlichen Angaben nach einem von dem Landesamt zu bestimmenden Meldeverfahren.

(2) Der Inhalt der nach diesem Gesetz vorgeschriebenen öffentlichen Bekanntmachungen kann zusätzlich im Internet veröffentlicht werden. Statt einer Anschrift ist nur der Wohnort, statt eines Geburtsdatums nur das Geburtsjahr anzugeben. Der Wahlleiter leitet den Inhalt der Bekanntmachungen nach § 9 Abs. 6 und § 18 Abs. 1 an das Landesamt für Statistik weiter. Dieses informiert die Öffentlichkeit im Internet unter www.wahlen.thueringen.de über die Wahlen."

3. Dem § 41 a wird folgender Absatz 3 angefügt:

"(3) Für Wahlverfahren nach diesem Gesetz, bei denen am 25. Mai 2018 bereits ein Wahltag festgesetzt war, ist das Thüringer Kommunalwahlgesetz in der am 24. Mai 2018 geltenden Fassung anzuwenden."

4. Die Inhaltsübersicht wird der vorstehenden Änderung angepasst.

Artikel 6
Änderung des Thüringer Beamtengesetzes

Das Thüringer Beamtengesetz vom 12. August 2014 (GVBl. S. 472), zuletzt geändert durch Artikel 3 des Gesetzes vom 24. April 2017 (GVBl. S. 91), wird wie folgt geändert:

1. § 72 Abs. 7 wird wie folgt geändert:

a) In Satz 1 wird die Angabe "§ 8 des Thüringer Datenschutzgesetzes (ThürDSG) in der Fassung vom 13. Januar 2012 (GVBl. S. 27) in der jeweils geltenden Fassung weitergeben" durch die Angabe "Artikels 28 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Ver-

arbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) übermitteln" ersetzt.

- b) In Satz 2 werden die Worte "und nutzen" gestrichen.

2. § 79 wird wie folgt geändert:

- a) In Absatz 1 Satz 1 werden die Worte "Personalplanung und des Personaleinsatzes" durch die Worte "Personalverwaltung und Personalwirtschaft" ersetzt.

- b) Absatz 2 erhält folgende Fassung:

"(2) Personalaktendaten dürfen in Dateien nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet werden. Darüber hinaus ist eine Verarbeitung zu anderen Zwecken in Übereinstimmung mit Artikel 6 Abs. 4 oder Artikel 88 Abs. 1 der Verordnung (EU) 2016/679 zulässig. Ein automatisierter Datenabruf durch andere Behörden ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist."

- c) In Absatz 4 Satz 1 wird das Wort "automatisierter" durch die Worte "im Wege des automatisierten Verfahrens erfolgter" ersetzt.

- d) In Absatz 5 wird das Wort "automatisiert" durch die Worte "im Wege des automatisierten Verfahrens" ersetzt.

3. § 80 wird wie folgt geändert:

- a) Nach Absatz 1 wird folgender neue Absatz 2 eingefügt:

"(2) Auftragsdatenverarbeitung ist im Rahmen der Artikel 28 und 29 der Verordnung (EU) 2016/679 zulässig."

- b) Der bisherige Absatz 2 wird Absatz 3 und Satz 1 erhält folgende Fassung:

"Dem Datenschutzbeauftragten nach § 13 des Thüringer Datenschutzgesetzes (ThürDSG) ist auf Verlangen mit Einwilligung der betroffenen Beamten Zugang zu den Personalakten zu gewähren."

4. § 81 wird wie folgt geändert:

- a) In Absatz 1 Satz 3 wird das Wort "bearbeitet" durch das Wort "verarbeitet" ersetzt.

- b) Absatz 2 erhält folgende Fassung:

"(2) Die Personalakten können nach sachlichen Gesichtspunkten in Grundakte und Teilakten gegliedert und in Teilen oder vollständig im Wege des automatisierten Verfahrens geführt werden. Teilakten kön-

nen bei der für den betreffenden Aufgabenbereich zuständigen Behörde geführt werden. Nebenakten mit Unterlagen, die sich auch in der Grundakte oder in Teilakten befinden, dürfen nur geführt werden, wenn die personalverwaltende Behörde nicht zugleich Beschäftigungsbehörde ist oder wenn mehrere personalverwaltende Behörden für die Beamten zuständig sind. In die Grundakte ist ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen. Werden die Personalakten nicht vollständig in Schriftform oder nicht vollständig im Wege des automatisierten Verfahrens geführt, legt die personalverwaltende Stelle jeweils schriftlich fest, welche Teile in welcher Form geführt werden und nimmt dies in das Verzeichnis nach Satz 4 auf."

5. Die §§ 83 und 84 erhalten folgende Fassung:

"§ 83
Anhörung

Ist beabsichtigt, Beschwerden, Behauptungen und Bewertungen, die für die Beamten ungünstig sind oder ihnen nachteilig werden können, in die Personalakte aufzunehmen, so sind die betroffenen Beamten darüber zu informieren. Ihnen ist Gelegenheit zur Stellungnahme zu geben, soweit die Anhörung nicht bereits nach anderen Rechtsvorschriften erfolgt. Ihre Äußerungen sind zur Personalakte zu nehmen.

§ 84
Auskunft an die betroffenen Beamten

(1) Der Anspruch der Beamten auf Auskunft aus ihren vollständigen Personalakten oder aus anderen Akten, die personenbezogene Daten enthalten, kann auch in Form der Einsichtnahme gewährt werden. Die personalaktenführende Stelle bestimmt, wo Einsichtnahme gewährt wird. Soweit dienstliche Gründe nicht entgegenstehen, können Auszüge, Abschriften, Ablichtungen oder Ausdrucke gefertigt werden. Beamten ist auf Verlangen ein Ausdruck der zu ihrer Person automatisiert gespeicherten Personalaktendaten zu überlassen.

(2) Bevollmächtigten von Beamten ist Auskunft zu gewähren, soweit dienstliche Gründe nicht entgegenstehen. Dies gilt auch für Hinterbliebene und deren Bevollmächtigte, wenn ein berechtigtes Interesse glaubhaft gemacht wird.

(3) Beamte haben ein Recht auf Einsicht auch in andere Akten, die personenbezogene Daten über sie enthalten und für ihr Dienstverhältnis verarbeitet werden, soweit gesetzlich nichts anderes bestimmt ist; dies gilt nicht für Sicherheitsakten. Die Einsichtnahme ist unzulässig, wenn die Daten der Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist den Beamten Auskunft zu erteilen."

6. § 85 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

"§ 85
Übermittlung von Personalaktendaten und
Auskünfte an Dritte"

b) Absatz 1 wird wie folgt geändert:

aa) In Satz 1 wird das Wort "vorzulegen" durch die Worte "zu übermitteln" ersetzt.

bb) In Satz 2 wird das Wort "Vorlage" durch das Wort "Übermittlung" ersetzt.

cc) In Satz 3 wird das Wort "genutzt" durch das Wort "verarbeitet" ersetzt.

dd) In Satz 4 wird das Wort "vorgelegt" durch das Wort "übermittelt" ersetzt.

ee) In Satz 6 wird das Wort "Vorlage" durch das Wort "Übermittlung" ersetzt.

c) Nach Absatz 1 wird folgender neue Absatz 2 eingefügt:

"(2) Die personalverwaltende Behörde kann mit Zustimmung der obersten Dienstbehörde Aufgaben, die ihr gegenüber den Beamten obliegen, auf eine andere Stelle übertragen. Dieser Stelle dürfen die zur Erfüllung der nach Satz 1 übertragenen Aufgaben erforderlichen Personalaktendaten übermittelt werden."

d) Die bisherigen Absätze 2 und 3 werden die Absätze 3 und 4.

e) Der bisherige Absatz 4 wird Absatz 5 und das Wort "Vorlage" wird durch das Wort "Übermittlung" ersetzt.

7. In § 86 Abs. 2 Satz 1 wird das Wort "drei" durch das Wort "zwei" ersetzt.

8. In § 87 Abs. 5 Satz 1 wird das Wort "automatisiert" durch die Worte "im Wege des automatisierten Verfahrens" ersetzt.

9. Die Inhaltsübersicht wird den vorstehenden Änderungen angepasst.

Artikel 7 Änderung des Thüringer Personalvertretungsgesetzes

In § 80 Abs. 2 des Thüringer Personalvertretungsgesetzes in der Fassung vom 13. Januar 2012 (GVBl. S. 1), das zuletzt durch Artikel 4 des Gesetzes vom 2. Juli 2016 (GVBl. S. 205, 212) geändert worden ist, wird die Verweisung "§ 37 des Thüringer Datenschutzgesetzes" durch die Verweisung "§ 6 des Thüringer Datenschutzgesetzes" ersetzt.

Artikel 8
Änderung des
Thüringer Informationsfreiheitsgesetzes

Das Thüringer Informationsfreiheitsgesetz vom 14. Dezember 2012 (GVBl. S. 464), zuletzt geändert durch Artikel 8 des Gesetzes vom 8. August 2014 (GVBl. S. 529), wird wie folgt geändert:

1. In § 6 Abs. 2 Satz 2 wird die Angabe "18. August 2009 (GVBl. S. 699)" durch die Angabe "1. Dezember 2014 (GVBl. S. 685)" ersetzt.
2. § 7 Abs. 4 wird aufgehoben.
3. § 9 Abs. 1 Satz 2 erhält folgende Fassung:

"Besondere Kategorien personenbezogener Daten nach Artikel 9 Abs. 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) dürfen nur zugänglich gemacht werden, wenn die betroffene Person ausdrücklich eingewilligt hat."

4. § 12 wird wie folgt geändert:

- a) Absatz 2 erhält folgende Fassung:

"(2) Dem Landesbeauftragten für die Informationsfreiheit ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; entsprechende Haushaltsmittel sind im Einzelplan des Landtags in einem eigenen Kapitel auszuweisen. Die Besetzung der Personalstellen erfolgt auf Vorschlag des Landesbeauftragten für die Informationsfreiheit. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit dem Landesbeauftragten für die Informationsfreiheit versetzt, abgeordnet oder umgesetzt werden; er ist ihr Dienstvorgesetzter, sie sind in ihrer Tätigkeit nach diesem Gesetz nur an seine Weisungen gebunden. Für bestimmte Einzelfragen kann der Landesbeauftragte für die Informationsfreiheit auch Dritte zur Mitarbeit heranziehen. Der Landesbeauftragte für die Informationsfreiheit

1. ist in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen,
2. steht zum Land nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis; der Präsident des Landtags führt die Dienstaufsicht, soweit nicht die Unabhängigkeit beeinträchtigt wird,
3. darf neben seinem Amt kein mit seiner Aufgabe nicht zu vereinbarendes anderes Amt ausüben,
4. darf kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des

- Bundes oder eines Landes angehören; er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben,
5. ist auch nach Beendigung seines Amtsverhältnisses verpflichtet, über die ihm bei 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,
 6. ist oberste Dienstbehörde im Sinne des § 96 der Strafprozessordnung sowie oberste Aufsichtsbehörde im Sinne des § 99 der Verwaltungsgerichtsordnung; er trifft die Entscheidungen über Aussagegenehmigungen für sich und seine Mitarbeiter sowie die Entscheidung über die Verweigerung der Aktenvorlage und der Auskunftserteilung in eigener Verantwortung. Der Nachfolger im Amt entscheidet über die genannten Entscheidungen für seine Vorgänger."

b) Absatz 4 Satz 2 erhält folgende Fassung:

"Er überwacht die Einhaltung dieses Gesetzes bei den in § 2 Abs. 1 genannten Stellen; er berät sie und kann Empfehlungen zur Verbesserung des Informationszugangs geben."

c) Folgender Absatz 7 wird angefügt:

"(7) Die Aufgabe des Landesbeauftragten für die Informationsfreiheit wird von dem Landesbeauftragten für den Datenschutz wahrgenommen. Der Landesbeauftragte für den Datenschutz kann sich auf seine institutionelle Garantie nach Artikel 69 der Verfassung des Freistaats Thüringen und seine Unabhängigkeit nach Artikel 52 der Verordnung (EU) 2016/679 berufen."

Artikel 9

Änderung des Thüringer Stiftungsgesetzes

In § 6 Abs. 2 des Thüringer Stiftungsgesetzes vom 16. Dezember 2008 (GVBl. S. 561), das zuletzt durch Artikel 2 des Gesetzes vom 13. März 2014 (GVBl. S. 92) geändert worden ist, werden die Worte "nicht den Antrag gestellt hat, auf die Angabe seines Namens zu verzichten" durch die Worte "hierzu schriftlich oder elektronisch eingewilligt hat" ersetzt.

Artikel 10

Änderung des Thüringer Rettungsdienstgesetzes

§ 30 des Thüringer Rettungsdienstgesetzes vom 16. Juli 2008 (GVBl. S. 233), das zuletzt durch Artikel 1 des Gesetzes vom 10. Juni 2014 (GVBl. S. 159) geändert worden ist, wird wie folgt geändert:

1. Absatz 1 erhält folgende Fassung:

"(1) Soweit sich aus diesem Gesetz nichts anderes ergibt, gelten für die am Rettungsdienst beteiligten Stellen die Bestimmungen der Verordnung (EU) 2016/679 des

Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) in Verbindung mit dem Thüringer Datenschutzgesetz."

2. In Absatz 2 werden die Worte "oder genutzt" gestrichen.
3. In Absatz 3 Nr. 1 und 2 wird jeweils das Wort "genutzt" durch das Wort "verwendet" ersetzt.
4. Absatz 4 Nr. 3 erhält folgende Fassung:

"3. zum Schutz der betroffenen Person oder zur Abwehr von Gefahren für die Rechte und Freiheiten einer anderen Person, sofern diese Gefährdung das Geheimhaltungsinteresse des Betroffenen überwiegt,"
5. Absatz 5 wird wie folgt geändert:
 - a) In der Einleitung wird das Wort "genutzt" durch das Wort "verwendet" ersetzt.
 - b) In Nummer 1 wird das Wort "nutzt" durch das Wort "verwendet" ersetzt.
 - c) In Nummer 2 werden die Worte "oder nutzen" gestrichen.

Artikel 11 **Änderung des Thüringer Vermessungs- und** **Geoinformationsgesetzes**

Das Thüringer Vermessungs- und Geoinformationsgesetz vom 16. Dezember 2008 (GVBl. S. 574), zuletzt geändert durch Artikel 1 und 3 des Gesetzes vom 30. Juli 2012 (GVBl. S. 355), wird wie folgt geändert:

1. In § 3 Abs. 2 Nr. 1 wird die Angabe "18. August 2009 (GVBl. S. 699)" durch die Angabe "1. Dezember 2014 (GVBl. S. 685)" ersetzt.
2. § 9 Abs. 7 wird wie folgt geändert:
 - a) Satz 4 erhält folgende Fassung:

"Auf Eigentumsangaben, die im Liegenschaftskataster in Übereinstimmung mit dem Grundbuch zu führen sind, finden die Artikel 16, 18 und 21 und auf Anschriften, Informationen über Bevollmächtigte der Eigentümer sowie über die Erben finden die Artikel 13, 14, 16, 18 und 21 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) keine Anwendung."

b) Folgender Satz wird angefügt:

"Satz 4 gilt nicht, wenn die betroffene Person fehlende Übereinstimmung der Eigentumsangaben mit dem Grundbuch geltend macht."

Artikel 12
**Änderung des Thüringer Hochschulgebühren-
und -entgeltgesetzes**

Das Thüringer Hochschulgebühren- und -entgeltgesetz vom 21. Dezember 2006 (GVBl. S. 601), zuletzt geändert durch Artikel 2 des Gesetzes vom 16. April 2014 (GVBl. S. 134), wird wie folgt geändert:

1. In § 4 Abs. 4 Nr. 1 wird die Angabe "6. Juni 1983 (BGBl. I S. 645, 1680)" durch die Angabe "7. Dezember 2010 (BGBl. I S. 1952, 2012 I S. 197)" ersetzt.
2. Nach § 5 Satz 2 wird folgender Satz eingefügt:

"Die Hochschulen sind berechtigt, die in diesem Zusammenhang für diese Zwecke erhobenen Daten zu verarbeiten."

Artikel 13
Änderung des Thüringer Schulgesetzes

Das Thüringer Schulgesetz in der Fassung vom 30. April 2003 (GVBl. S. 238), zuletzt geändert durch Artikel 5 des Gesetzes vom 31. Januar 2013 (GVBl. S. 22, 23), wird wie folgt geändert:

1. § 57 erhält folgende Fassung:

"§ 57
Datenschutz

(1) Zur Erfüllung der den Schulen, Schulträgern und Schulaufsichtsbehörden durch Rechtsvorschriften zugewiesenen Aufgaben ist das Verarbeiten personenbezogener Daten der Schüler, der Eltern sowie der Lehrer, der Erzieher und der Sonderpädagogischen Fachkräfte zulässig, soweit dies für den jeweils mit den Aufgaben verbundenen Zweck erforderlich ist.

(2) Die Schüler, die Eltern sowie die Lehrer, die Erzieher und die Sonderpädagogischen Fachkräfte sind verpflichtet, die erforderlichen Angaben zu machen.

(3) Im Rahmen der Schulgesundheitspflege dürfen für die Durchführung der schulärztlichen Untersuchungen die erforderlichen personenbezogenen Daten verarbeitet werden. Der schulärztliche Dienst darf der Schule nur das Ergebnis der Pflichtuntersuchungen übermitteln, sofern keine rechtswirksame Einwilligung der betroffenen Person vorliegt.

(4) Im Rahmen des Kinderschutzes nach § 55a Abs. 2 darf bei Anzeichen von Vernachlässigung, Misshandlung, sexuellem Missbrauch oder einer sonstigen ernsthaften Gefährdung des Wohls eines Schülers das mit der Aufklärung befasste Personal der Schule für eine Dokumentation die erforderlichen personenbezogenen Daten verarbeiten.

(5) Wissenschaftliche Forschungsvorhaben in Schulen bedürfen der Genehmigung des für das Schulwesen zuständigen Ministeriums. Die Genehmigung kann erteilt werden, wenn das Vorhaben ein erhebliches wissenschaftliches Interesse im Hinblick auf den Bildungsauftrag der Schule erkennen lässt und sich die Belastung der Schule in einem zumutbaren Rahmen hält. Personenbezogene Daten dürfen nur für ein bestimmtes Vorhaben verarbeitet werden, soweit die betroffenen Personen eingewilligt haben oder das öffentliche Interesse an der Durchführung des Vorhabens das Geheimhaltungsinteresse erheblich überwiegt und der Forschungszweck des Vorhabens auf eine andere Weise nicht oder nur mit einem unverhältnismäßigen Aufwand erreicht werden kann.

(6) Für internationale, nationale und regionale Vergleichsuntersuchungen, die auf Veranlassung des für das Schulwesen zuständigen Ministeriums in Schulen durchgeführt werden, können geeignete und erforderliche Testverfahren eingesetzt und insbesondere durch Befragung erforderliche Daten verarbeitet werden. Absatz 5 Satz 3 gilt entsprechend. Für die internen und externen Evaluationen zur Qualitätsentwicklung und Qualitätssicherung der Schulen sind die Sätze 1 und 2 entsprechend anzuwenden.

(7) Umfragen ohne Auskunftspflicht können für schulorganisatorische Aufgaben durch den Schulleiter durchgeführt werden.

(8) Das Nähere über das Verarbeiten personenbezogener Daten, insbesondere

1. über die bei der Aufnahme in die Schule, beim Schulwechsel und bei vergleichbaren Anlässen zu erhebenden oder zu übermittelnden Daten,
 2. das Führen und den Inhalt von Schülerakten und von Klassen- und Kursbüchern sowie den Umfang personenbezogener Angaben nach Absatz 6,
 3. den Einsatz automatisierter Verfahren auf Abruf,
 4. die erforderlichen Datensicherungsmaßnahmen und Aufbewahrungsfristen sowie
 5. das Verarbeiten von personenbezogenen Daten der Schüler durch den Lehrer auf dessen privaten Datenverarbeitungsgeräten außerhalb der Schule,
- wird durch Rechtsverordnung des für das Schulwesen zuständigen Ministeriums geregelt.

(9) Soweit in diesem Gesetz nichts anderes geregelt ist, gelten die Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) in Verbindung mit dem Thüringer Datenschutzgesetz."

2. § 58 wird wie folgt geändert:

- a) In Absatz 1 Satz 1 werden die Worte "Erheben und" gestrichen.
- b) In Absatz 3 werden die Worte "Erheben, Verarbeiten und Nutzen" durch das Wort "Verarbeiten" ersetzt.

3. § 60 Satz 1 wird wie folgt geändert:

- a) In Nummer 16 werden die Worte "Erhebung und" gestrichen.
- b) In Nummer 17 werden die Worte "bei der Erhebung und Verarbeitung" durch die Worte "bei der Verarbeitung" ersetzt.

Artikel 14

Änderung des Thüringer Gesetzes zur Ausführung des Artikel 10-Gesetzes

In § 3 Abs. 2 Satz 1 des Thüringer Gesetzes zur Ausführung des Artikel 10-Gesetzes vom 16. Juli 2008 (GVBl. S. 245), das durch Artikel 3 des Gesetzes vom 21. Dezember 2011 (GVBl. S. 530) geändert worden ist, werden die Worte "Erhebung, Verarbeitung und Nutzung" durch das Wort "Verarbeitung" ersetzt.

Artikel 15

Änderung des Thüringer Verfassungsschutzgesetzes

Das Thüringer Verfassungsschutzgesetz vom 8. August 2014 (GVBl. S. 529) wird wie folgt geändert:

1. § 2 Abs. 5 wird wie folgt geändert:

- a) In Satz 2 Nr. 7 wird das Wort "Weiterleitung" durch das Wort "Übermittlung" ersetzt.
- b) In Satz 3 wird das Wort "Verwaltungsvorschrift" durch das Wort "Dienstvorschrift" ersetzt.

2. § 6 Abs. 2 wird wie folgt geändert:

- a) Nummer 4 wird aufgehoben.
- b) Die bisherigen Nummern 5 bis 8 werden die Nummern 4 bis 7.

3. In § 7 Abs. 1 Satz 1 werden die Worte "und nutzen, namentlich speichern, übermitteln, verändern, löschen und abgleichen" gestrichen sowie nach dem Wort "entgegenstehen" ein Semikolon und die Worte "die Verarbeitung ist auch zulässig, wenn der Betroffene eingewilligt hat" eingefügt.

4. § 8 wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

aa) Satz 3 erhält folgende Fassung:

"Für Auskünfte der Verpflichteten nach Absatz 1 und 2 an das Amt für Verfassungsschutz gelten die aufgrund von § 8b Abs. 8 Satz 1 bis 3 des Bundesverfassungsschutzgesetzes (BVerfSchG) vom 20. Dezember 1990 (BGBl. I S. 2954 -2970-) in der jeweils geltenden Fassung erlassene Rechtsverordnung sowie die Vorgaben nach § 8b Abs. 8 Satz 4 und 5 BVerfSchG in der jeweils geltenden Fassung entsprechend."

bb) Folgender Satz wird angefügt:

"Im Übrigen gilt § 8b Abs. 4 bis 6 BVerfSchG für besondere Auskunftsverlangen des Amtes für Verfassungsschutz entsprechend."

b) Nach Absatz 2 wird folgender Absatz 2 a eingefügt:

"(2 a) Für die Einholung von Auskünften über das Bundeszentralamt für Steuern durch das Amt für Verfassungsschutz gilt § 8a Abs. 2a BVerfSchG entsprechend. Über die Einholung der Auskünfte entscheidet der Präsident oder sein Stellvertreter."

c) In Absatz 4 Satz 5 werden die Worte "Erhebung, Verarbeitung und Nutzung" durch das Wort "Verarbeitung" ersetzt.

5. § 13 Abs. 3 wird wie folgt geändert:

a) In Satz 1 werden die Worte "speichern, verarbeiten und nutzen" durch das Wort "verarbeiten" ersetzt.

b) In Satz 2 werden die Worte "Speicherung, Verarbeitung und Nutzung" durch das Wort "Verarbeitung" ersetzt.

c) In Satz 3 werden die Worte "weitere Verarbeitung oder Nutzung" durch die Worte "Abfrage und Verwendung" ersetzt.

6. In § 16 Abs. 1 Nr. 3 werden die Worte "und Nutzung" gestrichen.

7. § 18 Abs. 1 Satz 1 wird wie folgt geändert:

a) In Nummer 2 wird das abschließende Komma durch einen Punkt ersetzt.

b) Nummer 3 wird aufgehoben.

8. In § 22 Abs. 2 wird die Verweisung "§ 5 Abs. 1 oder 3 Bundesverfassungsschutzgesetz" durch die Verweisung "§ 6 BVerfSchG" ersetzt.

9. § 36 erhält folgende Fassung:

"§ 36
Geltung des Thüringer Datenschutzgesetzes

Bei der Erfüllung der Aufgaben nach § 4 durch das Amt für Verfassungsschutz finden § 2 Abs. 1, 2 und 4 Satz 1, Abs. 6 bis 9, die §§ 3 bis 6, § 7 Abs. 2 bis 6, die §§ 8, 10 bis 17 Abs. 1, die §§ 18, 32, 39 Abs. 1 bis 4, § 42 Abs. 1 Satz 2, Abs. 2 und 3 sowie die §§ 48, 49 und 54 des Thüringer Datenschutzgesetzes entsprechend Anwendung."

Artikel 16
Änderung des
Thüringer Sicherheitsüberprüfungsgesetzes

Das Thüringer Sicherheitsüberprüfungsgesetz vom 17. März 2003 (GVBl. S. 185), zuletzt geändert durch Ar-

tikel 2 des Gesetzes vom 8. August 2014 (GVBl. S. 529), wird wie folgt geändert:

1. In § 6 Abs. 3 Satz 4 wird die Angabe "§ 37 Abs. 2 des Thüringer Datenschutzgesetzes in der Fassung vom 13. Januar 2012 (GVBl. S. 27) in der jeweils geltenden Fassung" durch die Angabe "§ 7 Abs. 3 des Thüringer Datenschutzgesetzes" ersetzt.
2. In § 22 Abs. 4 Satz 2 werden die Worte "verarbeiten und nutzen" durch die Worte "speichern, nutzen, verändern und übermitteln" ersetzt.
3. § 23 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

"§ 23
Berichtigung, Löschung und Einschränkung der
Verarbeitung personenbezogener Daten"

b) Absatz 3 wird wie folgt geändert:

aa) In Satz 2 werden die Worte "zu sperren" durch die Worte "in der Verarbeitung einzuschränken" ersetzt.

bb) In Satz 3 wird das Wort "genutzt" durch die Worte "gespeichert, genutzt, verändert, übermittelt und gelöscht" ersetzt.

4. In § 24 Abs. 4 Satz 3 bis 6 werden jeweils die Worte "Landesbeauftragten für Datenschutz" durch die Worte "Landesbeauftragten für den Datenschutz" ersetzt.
5. § 36 wird wie folgt geändert:

a) Die Überschrift erhält folgende Fassung:

"§ 36
Übergangsbestimmungen, Geltung des
Thüringer Datenschutzgesetzes"

b) Folgender Absatz 3 wird angefügt:

"(3) § 2 Abs. 1, 2 und 4 Satz 1, Abs. 6 bis 9, die §§ 3 bis 6, § 7 Abs. 2 bis 6, die §§ 8, 10 bis 17 Abs. 1, die §§ 18, 32, 39 Abs. 1 und 3 sowie die §§ 48, 49 und 54 des Thüringer Datenschutzgesetzes finden entsprechende Anwendung."

6. Die Inhaltsübersicht wird den vorstehenden Änderungen angepasst.

Artikel 17 Änderung des Thüringer Statistikgesetzes

Das Thüringer Statistikgesetz vom 21. Juli 1992 (GVBl. S. 368), zuletzt geändert durch Artikel 3 des Gesetzes vom 25. November 2004 (GVBl. S. 853), wird wie folgt geändert:

1. § 3 Satz 1 erhält folgende Fassung:

"Werden für eine Statistik, die von einer öffentlichen Stelle durchgeführt wird, Einzelangaben verarbei-

tet, gelten die Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) in Verbindung mit den §§ 3 bis 12 und 19 Thüringer Datenschutzgesetz (ThürDSG)."

2. § 18 Abs. 5 Satz 1 erhält folgende Fassung:

"Für die Durchführung wissenschaftlicher Vorhaben darf das Landesamt Einzelangaben an Hochschulen oder sonstige Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung übermitteln."

3. § 19 wird wie folgt geändert:

a) In der Einleitung werden nach dem Wort "elektronisch" die Worte "neben den Informationen nach Artikel 13 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72)" eingefügt.

b) Nummer 1 erhält folgende Fassung:

"1. Art und Umfang der Erhebung;"

Artikel 18

Änderung des Thüringer Gesetzes zur Ausführung der Verwaltungsgerichtsordnung

§ 8 c des Thüringer Gesetzes zur Ausführung der Verwaltungsgerichtsordnung in der Fassung vom 15. Dezember 1992 (GVBl. S. 576), das zuletzt durch Artikel 6 des Gesetzes vom 8. August 2014 (GVBl. S. 527) geändert worden ist, wird aufgehoben.

Artikel 19

Änderung des Thüringer Gesetzes zur Umsetzung der Bestimmungen über die europäische Amtshilfe

In § 5 Satz 1 des Thüringer EU-Amtshilfegesetzes vom 8. Juli 2009 (GVBl. S. 592), zuletzt geändert durch Artikel 11 des Gesetzes vom 2. Juli 2016 (GVBl. S. 229), werden die Worte "erheben, speichern, übermitteln und nutzen" durch das Wort "verarbeiten" ersetzt.

Artikel 20

Änderung des Thüringer Tiergesundheitsgesetzes

In § 35 Satz 1 des Thüringer Tiergesundheitsgesetzes in der Fassung vom 30. März 2010 (GVBl. S. 89), das zuletzt durch Artikel 1 des Gesetzes vom 28. Oktober 2013 (GVBl. S. 299) geändert worden ist, werden die Worte "und zu nutzen" gestrichen.

Artikel 21**Änderung des Thüringer Landesmediengesetzes**

Das Thüringer Landesmediengesetz vom 15. Juli 2014 (GVBl. S. 385), geändert durch Artikel 2 des Gesetzes vom 23. September 2015 (GVBl. S. 134), wird wie folgt geändert:

1. § 6 erhält folgende Fassung:

"§ 6

Datenverarbeitung zu journalistischen Zwecken,
Medienprivileg

(1) Soweit Veranstalter von landesweitem, regionalem und lokalem Rundfunk sowie landesweit, regional und lokal ausgerichtete Anbieter von Telemedien personenbezogene Daten zu journalistischen Zwecken verarbeiten, ist es den hiermit befassten Personen untersagt, diese Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Im Übrigen finden für die Datenverarbeitung zu journalistischen Zwecken von der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz der natürlichen Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) außer den Kapiteln I, VIII, X und XI nur Artikel 5 Abs. 1 Buchst. f in Verbindung mit Abs. 2, Artikel 24 und Artikel 32 Anwendung. Artikel 82 der Verordnung (EU) 2016/679 gilt mit der Maßgabe, dass nur für eine Verletzung des Datengeheimnisses gemäß der Sätze 1 bis 3 sowie für unzureichende Maßnahmen nach Artikel 5 Abs. 1 Buchst. f sowie den Artikeln 24 und 32 der Verordnung (EU) 2016/679 gehaftet wird. Die Sätze 1 bis 5 gelten entsprechend für die zu den in Satz 1 genannten Stellen gehörenden Hilfs- und Beteiligungsunternehmen. Die Veranstalter von landesweitem, regionalem und lokalem Rundfunk sowie landesweit, regional und lokal ausgerichtete Anbieter von Telemedien können sich Verhaltenskodizes geben, die in einem transparenten Verfahren erlassen und veröffentlicht werden. Den betroffenen Personen stehen nur die in den Absätzen 2 und 3 genannten Rechte zu.

(2) Führt die journalistische Verarbeitung personenbezogener Daten zur Verbreitung von Gegendarstellungen der betroffenen Person oder zu Verpflichtungserklärungen, Beschlüssen oder Urteilen über die Unterlassung der Verbreitung oder über den Widerruf des Inhalts der Daten, so sind diese Gegendarstellungen, Verpflichtungserklärungen und Widerrufe zu den gespeicherten Daten zu nehmen und dort für dieselbe Zeitdauer aufzubewahren wie die Daten selbst sowie bei einer Übermittlung der Daten gemeinsam mit diesen zu übermitteln.

(3) Wird jemand durch eine Berichterstattung in seinem Persönlichkeitsrecht beeinträchtigt, kann die betroffene Person Auskunft über die der Berichterstattung zu

Gründe liegenden zu ihrer Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunk- sendungen mitwirken oder mitgewirkt haben, geschlossen werden kann,
2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann oder
3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe durch Ausforschung des Informationsbestandes beeinträchtigt würde.

Die betroffene Person kann die unverzügliche Berichtigung unrichtiger personenbezogener Daten im Datensatz oder die Hinzufügung einer eigenen Darstellung von angemessenem Umfang verlangen. Die weitere Speicherung der personenbezogenen Daten ist rechtmäßig, wenn dies für die Ausübung des Rechts auf freie Meinungsäußerung und Information oder zur Wahrnehmung berechtigter Interessen erforderlich ist.

(4) Die Absätze 1 bis 3 gelten auch für Teleshoppingkanäle.

(5) Der Landesbeauftragte für den Datenschutz überwacht die Einhaltung der Datenschutzvorschriften im Anwendungsbereich dieses Gesetzes. Festgestellte Verletzungen von Bestimmungen über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten werden der Landesmedienanstalt mitgeteilt, damit diese die nach diesem Gesetz vorgesehenen Maßnahmen treffen kann.

(6) Dem Landesbeauftragten für den Datenschutz stehen gegenüber den nicht öffentlichen Stellen die in § 40 Abs. 3 bis 5 des Bundesdatenschutzgesetzes genannten Rechte in Verbindung mit § 11 des Thüringer Datenschutzgesetzes zu."

2. Die Inhaltsübersicht wird den vorstehenden Änderungen angepasst.

Artikel 22

Änderung des Thüringer Pressegesetzes

§ 11 a des Thüringer Pressegesetzes vom 31. Juli 1991 (GVBl. S. 271), das zuletzt durch Artikel 3 des Gesetzes vom 16. Juli 2008 (GVBl. S. 243) geändert worden ist, erhält folgende Fassung:

"§ 11 a

Datenverarbeitung zu journalistischen und literarischen Zwecken, Medienprivileg

Soweit Unternehmen und Hilfsunternehmen der Presse personenbezogene Daten zu journalistischen oder literarischen Zwecken verarbeiten, ist es den hiermit befassten Personen untersagt, diese personenbezogenen Daten zu anderen Zwecken zu verarbeiten (Datengeheimnis). Die-

se Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort. Im Übrigen finden für die Datenverarbeitung zu journalistischen oder literarischen Zwecken von den Kapiteln II bis VII und IX der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz der natürlichen Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) nur Artikel 5 Abs. 1 Buchst. f und Artikel 24 sowie § 83 des Bundesdatenschutzgesetzes (BDSG) Anwendung. Artikel 82 der Verordnung (EU) 2016/679 und § 83 BDSG gelten mit der Maßgabe, dass nur für eine Verletzung des Datengeheimnisses nach Satz 1 und für unzureichende Maßnahmen nach Artikel 5 Abs. 1 Buchst. f und Artikel 24 der Verordnung (EU) 2016/679 gehaftet wird."

Artikel 23

Änderung des Thüringer Gesetzes über das Verfahren bei Einwohnerantrag, Bürgerbegehren und Bürgerentscheid

Das Thüringer Gesetz über das Verfahren bei Einwohnerantrag, Bürgerbegehren und Bürgerentscheid vom 7. Oktober 2016 (GVBl. S. 506, 691), geändert durch Gesetz vom 28. Juni 2017 (GVBl. S. 157), wird wie folgt geändert:

1. § 5 wird wie folgt geändert:
 - a) In Absatz 1 Satz 1 werden die Worte "und genutzt" gestrichen.
 - b) In Absatz 2 werden die Worte "oder nutzt" gestrichen.
2. In § 6 Abs. 2 Satz 1 werden die Worte "und genutzt" gestrichen.

Artikel 24

Änderung des Thüringer Berufsqualifikationsfeststellungsgesetzes

Das Thüringer Berufsqualifikationsfeststellungsgesetz vom 16. April 2014 (GVBl. S. 139), geändert durch Artikel 1 des Gesetzes vom 2. Juli 2016 (GVBl. S. 229), wird wie folgt geändert:

1. In § 1 Satz 2 wird der Klammerzusatz "(ABl. L 255 vom 30.9.2005, S. 22; L 271 vom 16.10.2007, S. 18; L 93 vom 4.4.2008, S. 28; L 33 vom 3.2.2009, S. 49)" durch den Klammerzusatz "(ABl. L 255 vom 30.9.2005, S. 22; L 271 vom 16.10.2007, S. 18; L 93 vom 4.4.2008, S. 28; L 33 vom 3.2.2009, S. 49; L 305 vom 24.10.2014, S. 115)" ersetzt.
2. § 13 b wird wie folgt geändert:
 - a) Absatz 4 wird aufgehoben.
 - b) Der bisherige Absatz 5 wird Absatz 4.

- c) Der bisherige Absatz 6 wird Absatz 5 und die Verweisung "Absatz 5" wird durch die Verweisung "Absatz 4" ersetzt.
- d) Die bisherigen Absätze 7 und 8 werden die Absätze 6 und 7.
3. In § 16 Abs. 6 Nr. 2 Halbsatz 2 werden das Wort "Arten" durch das Wort "Kategorien" und die Verweisung "§ 3 Abs. 1 Thüringer Datenschutzgesetz (ThürDSG) in der Fassung vom 13. Januar 2012 (GVBl. S. 27) in der jeweils geltenden Fassung" durch die Verweisung "Artikel 9 Abs. 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72)" ersetzt.

Artikel 25

Änderung des Thüringer Bestattungsgesetzes

§ 15 Abs. 4 Satz 2 des Thüringer Bestattungsgesetzes vom 19. Mai 2004 (GVBl. S. 505), das zuletzt durch Artikel 1 des Gesetzes vom 22. November 2016 (GVBl. S. 518) geändert worden ist, erhält folgende Fassung:

"Im Fall der Übermittlung von Daten nach Satz 1 Nr. 2 gelten die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) und § 18 in Verbindung mit § 17 Abs. 2 Satz 2 sowie § 28 des Thüringer Datenschutzgesetzes entsprechend."

Artikel 26

Änderung des Thüringer Laufbahngesetzes

§ 25 des Thüringer Laufbahngesetzes vom 12. August 2014 (GVBl. S. 472, 498), das zuletzt durch Artikel 4 des Gesetzes vom 24. April 2017 (GVBl. S. 91, 94) geändert worden ist, wird wie folgt geändert:

1. In Absatz 1 Satz 1 Nr. 1 wird der Klammerzusatz "(ABl. L 255 vom 30.9.2005, S. 22; L 271 vom 16.10.2007, S. 18; L 93 vom 4.4.2008, S. 28; L 33 vom 3.2.2009, S. 49; L 354 vom 28.12.2013, S. 132)" durch den Klammerzusatz "(ABl. L 255 vom 30.9.2005, S. 22; L 271 vom 16.10.2007, S. 18; L 93 vom 4.4.2008, S. 28; L 33 vom 3.2.2009, S. 49; L 305 vom 24.10.2014, S. 115)" ersetzt.
2. In Absatz 4 Satz 1 wird die Verweisung "§ 13b Abs. 1 bis 5 und 7" durch die Verweisung "§ 13b Abs. 1 bis 4 und 6" ersetzt.

Artikel 27

Inkrafttreten, Außerkrafttreten

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

(2) Gleichzeitig mit dem Inkrafttreten nach Absatz 1 tritt das Thüringer Datenschutzgesetz vom 13. Januar 2001 (GVBl. S. 27), zuletzt geändert durch Artikel 7 des Gesetzes vom 8. August 2014 (GVBl. S. 539, 544), außer Kraft.

Begründung:

Mit der Neufassung des Thüringer Datenschutzgesetzes sowie der Umstrukturierung der weiteren Fachgesetze werden die europarechtlichen Vorgaben der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 im Thüringer Datenschutzrecht umgesetzt.

Zu Artikel 1**Thüringer Datenschutzgesetz (ThürDSG)****Zum Ersten Abschnitt****Gemeinsame Bestimmungen****Zum Ersten Unterabschnitt****Allgemeine Bestimmungen**

Durch dieses Gesetz werden die für die Umsetzung notwendigen und möglichen ergänzenden Regelungen zur Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) (Verordnung (EU) 2016/679) durchgesetzt. Der Gesetzeszweck wird dem Gesetz vorangestellt, um deutlich zu machen, dass das Thüringer Datenschutzgesetz nur in Ergänzung zur Verordnung (EU) 2016/679 gilt und nur gemeinsam mit ihr richtig angewendet werden kann.

Dabei erfolgt im Ersten Abschnitt eine Umsetzung allgemeiner Regelungen, die zugleich auch Vorgaben der Richtlinie (EU) 2016/680 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 Strafverfolgung und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) (Richtlinie (EU) 2016/680) verwirklichen, da beide Regelungen soweit wort- oder inhaltsgleich sind.

Demgegenüber dient der Zweite Abschnitt ausschließlich der Umsetzung der Verordnung (EU) 2016/679. Infolge der unmittelbaren Geltung der Verordnung (EU) 2016/679 ist diese in Teilen direkt und ohne Umsetzungsakt anwendbar. Die Bundesrepublik Deutschland als Mitgliedstaat der Europäischen Union und damit auch die Bundesländer sind insofern verpflichtet, die Verordnung (EU) 2016/679 zu beachten und zu vollziehen. Aufgrund des Anwendungsvorrangs der Verordnung (EU) 2016/679 werden die Bestimmungen des bisherigen Thüringer Datenschutzgesetzes vom 13. Januar 2012 (GVBl. S. 27), zuletzt geändert durch Artikel 7 des Gesetzes vom 8. August 2014 (GVBl. S. 539, 544) -ThürDSG a. F.- verdrängt. Teilweise sind die nationalen Gesetzgeber aber auch verpflichtet, Regelungen der Verordnung im eigenen Recht umzusetzen oder die Verordnung (EU) 2016/679 räumt die Möglichkeit ein, von ihren Vorgaben unter bestimmten und benannten Voraussetzungen abzuweichen. Dieses Gesetz ergänzt daher auch die Verordnung (EU) 2016/679 und hält in Teilen bisherige Datenschutzstandards aufrecht, indem Bestimmungen des ThürDSG a. F. in das neue Regelungssystem integriert werden. Das Gesetz kommt damit einerseits den in der Verordnung (EU) 2016/679 enthaltenen Regelungsaufträgen nach und nutzt andererseits die dort enthaltenen Regelungsoptionen im Hinblick auf die Datenverarbeitung durch öffentliche Stellen des Landes. Das Thüringer Datenschutzgesetz erhält daher eine völlig neue Struktur. Sofern Bestimmungen des bisherigen Rechts in diesem Gesetz übernom-

men wurden, findet sich eine entsprechende Begründung in den einzelnen Bestimmungen.

Der Dritte Abschnitt dient der Umsetzung der Richtlinie (EU) 2016/680, sofern Bestimmungen nicht in spezialgesetzlichen Regelungen verortet werden (Beispiel Polizeiaufgabengesetz).

Der Vierte Abschnitt enthält Regelungen zu Ordnungswidrigkeiten und Strafbestimmungen im Anwendungsbereich der Verordnung (EU) 2016/679 sowie des § 31. Im Fünften Abschnitt werden schließlich Ausnahmeregelungen für Datenverarbeitungen getroffen, welche nicht in den Anwendungsbereich der Verordnung (EU) 2016/679 fallen, auf welche ihre Regelungen sowie diejenigen dieses Gesetzes aber dennoch anzuwenden sind, soweit im Fünften Abschnitt keine Regelungen getroffen wurden.

Zu § 1

Zweck des Gesetzes

Dieses Gesetz dient der Umsetzung der notwendigen ergänzenden Regelungen zur Verordnung (EU) 2016/679.

Da das Datenschutzrecht auch im Anwendungsbereich der Richtlinie (EU) 2016/680 reformiert wurde und europarechtliche Richtlinien dem nationalen Gesetzgeber regelmäßig größere Umsetzungsspielräume belassen als eine Verordnung, hat sich der Thüringer Gesetzgeber dafür entschieden, in diesem Gesetz auch Teile der Richtlinie (EU) 2016/680 umzusetzen. Absatz 2 macht dies deutlich.

Dabei werden im Ersten und Vierten Abschnitt allgemeine Bestimmungen sowohl der Verordnung (EU) 2016/679 als auch der Richtlinie (EU) 2016/680 und im Zweiten Abschnitt Bestimmungen der Verordnung (EU) 2016/679 umgesetzt, während im Dritten Abschnitt ausschließlich spezielle Vorgaben der Richtlinie (EU) 2016/680 umgesetzt werden, die aufgrund ihres speziellen Inhalts nicht mit der Verordnung (EU) 2016/679 gemeinsam umgesetzt werden konnten.

Zu § 2

Anwendungsbereich

Zu Absatz 1 und 2:

Die Absätze 1 und 2 entsprechen den bisherigen Regelungen. Nach Absatz 1 gilt das Gesetz, wie bisher auch für die Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung. Welche öffentlichen Stellen darunter fallen, wird in Absatz 1 gesetzlich definiert. Für Gerichte ist zusätzlich Absatz 8 zu beachten, für Staatsanwaltschaften Absatz 9. Absatz 2 dient der Klarstellung und bestimmt angesichts der Praxis der Ausgliederung von Organisationseinheiten aus der öffentlichen Verwaltung, dass auch diese als öffentliche Stellen im Sinne dieses Gesetzes gelten.

Zu Absatz 3:

Um Wettbewerbsverzerrungen zu vermeiden, werden die in Absatz 3 explizit genannten Stellen denselben datenschutzrechtlichen Normen unterworfen wie nichtöffentliche Stellen. Insoweit gelten die Bestimmungen des Bundesdatenschutzgesetzes (BDSG), es sei denn durch Gesetz oder Staatsvertrag wird etwas anderes bestimmt.

Zu Absatz 4:

Absatz 4 bestimmt die Normenhierarchie im Anwendungsbereich dieses Gesetzes. Er definiert das Verhältnis des Gesetzes zu anderen fachspezifischen Bestimmungen auf Bundes- und Landesebene. Durch die Bestimmung wird sichergestellt, dass jede Datenverarbeitung durch öf-

fentliche Stellen im Anwendungsbereich des Gesetzes, der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 datenschutzrechtlich geregelt wird.

Satz 2 bestimmt, dass dieses Gesetz anzuwenden ist, soweit nicht durch das Fachrecht speziellere Regelungen getroffen wurden und schließt eine Regelungslücke für den Fall, dass spezialgesetzlich keine Regelung getroffen wurde. Dabei ist die aufgezeigte Systematik des § 1 zu beachten. Satz 3 entspricht der bisherigen Rechtslage. Durch Satz 3 wird sichergestellt, dass der Schutz spezieller Verwaltungszweige und Berufsgruppen durch spezifische gesetzliche und gesetzlich nicht kodifizierte Geheimhaltungspflichten durch dieses Gesetz nicht verringert wird.

Zu Absatz 5:

Absatz 5 regelt die Anwendbarkeit der Verordnung (EU) 2016/679 für die Verarbeitung personenbezogener Daten im Zusammenhang mit Sachverhalten, die zunächst nach Artikel 2 der Verordnung (EU) 2016/679 oder Artikel 2 der Richtlinie (EU) 2016/680 nicht in den jeweiligen Anwendungsbereich fallen.

Es handelt sich um eine konstitutiv wirkende Regelung, durch die sichergestellt wird, dass auch für die nicht unter die Verordnung (EU) 2016/679 oder die Richtlinie (EU) 2016/680 fallenden Bereiche entsprechend der bisherigen Regelungssystematik ein datenschutzrechtliches Vollregime besteht. Satz 2 enthält eine Klarstellung für ungeordnete Akten, die nach Artikel 2 Absatz 1 der Verordnung (EU) 2016/679 nicht in deren Anwendungsbereich fallen. Die Artikel 30, 35 und 36 der Verordnung (EU) 2016/679 sind in diesem Fall auch nicht entsprechend anwendbar.

Zu Absatz 6:

Absatz 6 entspricht der bisherigen Regelung. Das definierte Stufenverhältnis bleibt durch die Umsetzung der europäischen Datenschutzreform unverändert. Das Thüringer Verwaltungsverfahrensgesetz und Datenschutzrecht stehen gleichrangig nebeneinander. Dieses Gesetz ist aber, soweit personenbezogene Daten verarbeitet werden, das speziellere Gesetz und vorrangig anzuwenden.

Zu Absatz 7:

Absatz 7 entspricht der bisherigen Regelung. Die Bestimmungen dieses Gesetzes gelten für den Landtag als Organ der gesetzgebenden Gewalt nur, soweit er in Verwaltungsangelegenheiten tätig wird. Der Begriff "Verwaltungsangelegenheiten" wird dabei nicht abschließend definiert und umfasst neben den ausdrücklich genannten Sachverhalten unter anderem auch die Beschaffung und Verwaltung von Sachmitteln, die Führung von Adress- und Telefonverzeichnissen, die Öffentlichkeitsarbeit sowie die für die Durchführung dieser Tätigkeiten erforderlichen Hilfstätigkeiten. Kein Tätigwerden in Verwaltungsangelegenheiten liegt demgegenüber bei den durch Artikel 48 der Verfassung des Freistaats Thüringen dem Landtag zugewiesenen Aufgaben vor. In diesem Bereich gilt dieses Gesetz nicht.

Zu Absatz 8:

Absatz 8 macht deutlich, dass die Bestimmungen über die Datenschutzaufsicht nach §§ 3 bis 12, zum Datenschutzbeauftragten sowie zum Führen von Verzeichnissen aller Verarbeitungstätigkeiten nur im Rahmen von Verwaltungsangelegenheiten, nicht aber im Rahmen der justiziellen Tätigkeit beziehungsweise Prüftätigkeit der Gerichte und des Rechnungshofes anwendbar sind. Darüber hinaus gilt die Pflicht zum Führen von Verfahrensverzeichnissen auch dann nicht für die Gerichte, wenn sie an der Strafverfolgung, der Verfolgung von Ordnungswidrigkeiten

und der Vollstreckung mitwirken. Die übrigen Bestimmungen der Verordnung (EU) 2016/679 sowie dieses Gesetzes haben die Gerichte sowie der Rechnungshof allerdings stets zu beachten. Mit Absatz 8 soll die verfassungsrechtliche Trennung von Exekutive und Judikative klarstellend zum Ausdruck gebracht werden (vergleiche dazu die Stellung des Thüringer Rechnungshofs in Artikel 103 der Verfassung des Freistaats Thüringen sowie die Unabhängigkeit der Gerichte in Artikel 47 Abs. 3 der Verfassung des Freistaats Thüringen), die sich auch in Artikel 55 Abs. 3 der Verordnung (EU) 2016/679 wiederfindet. Die Vorschrift entspricht dem bisherigen Recht und stärkt die miteinander vergleichbare unabhängige Stellung sowie Funktion der Gerichte und des Rechnungshofs.

Zu Absatz 9:

Absatz 9 bestimmt, dass für die Staatsanwaltschaften neben dem stets anwendbaren Ersten Abschnitt im Rahmen ihrer allgemeinen Verwaltungstätigkeit die Regelungen des Zweiten und Vierten Abschnitts und im Rahmen von Tätigkeiten nach § 31 der Dritte und Vierte Abschnitt gelten.

Zum Zweiten Unterabschnitt Aufsichtsbehörde

Im Zweiten Unterabschnitt werden diejenigen Bestimmungen zum Thüringer Landesbeauftragten für den Datenschutz geregelt, welche aus der Verordnung (EU) 2016/679 folgen. Dabei ergibt sich bereits unmittelbar aus der Verordnung (EU) 2016/679, unter welchen Voraussetzungen das Amtsverhältnis des Landesbeauftragten endet (Artikel 53 Absatz 3 und 4), die erforderliche Qualifikation, die Weisungsungebundenheit (Artikel 52 Absatz 2) und die mit dem Amt nicht zu vereinbarenden Handlungen (Artikel 52 Absatz 3). Teilweise sieht die Verordnung (EU) 2016/679 dabei eine Konkretisierungspflicht der Mitgliedstaaten der Europäischen Union vor, so zur Amtszeit und zur Wiederwahlmöglichkeit (Artikel 54 Absatz 1 Buchst. d und e) sowie zur Qualifikation der Mitglieder der Aufsichtsbehörde (Artikel 54 Absatz 1 Buchst. b). Sofern dieses Gesetz zu den genannten Punkten keine Angaben macht, sind beamten- und tarifrechtliche Regelungen anwendbar.

Durch den Gesetzgeber sind nach der Verordnung darüber hinaus noch die Ausstattung (Artikel 52 Absatz 4), die Personalhoheit (Artikel 52 Absatz 5), die finanzielle Unabhängigkeit und die Finanzkontrolle (Artikel 52 Absatz 6), das Verfahren der Ernennung und Errichtung (Artikel 53 Absatz 1, Artikel 54 Absatz 1 Buchst. a, b und c) sowie die Pflichten der Mitglieder und Bediensteten der Aufsichtsbehörde (Artikel 54 Absatz 1 Buchst. f) sicherzustellen.

Zudem werden durch diesen Unterabschnitt die Vorgaben der Richtlinie (EU) 2016/680 an die Aufsichtsbehörde umgesetzt. Dem Gesetzgeber steht dabei grundsätzlich ein größerer Umsetzungsspielraum zu, als bei der Verordnung (EU) 2016/679. Im Interesse eines einheitlichen Rechtsrahmens werden dabei, sofern dies aufgrund der inhaltlichen Vorgaben beider Regime möglich ist, die Bestimmungen der Verordnung (EU) 2016/679 übernommen und angepasst. Sofern die Vorgaben der Verordnung (EU) 2016/679 denen der Richtlinie (EU) 2016/680 entsprechen, werden diese in Umsetzung der Richtlinie (EU) 2016/680 zitiert. Dies ist im Rahmen der Umsetzung der Richtlinie (EU) 2016/680 zulässig, da sie den Mitgliedstaaten der Europäischen Union insoweit Umsetzungsspielraum lässt und auch das unionsrechtliche Zitierverbot keine Anwendung findet.

Zu § 3**Landesbeauftragter für den Datenschutz (Artikel 51 bis 54 der Verordnung (EU) 2016/679, Artikel 41 bis 44 der Richtlinie (EU) 2016/680)**

§ 3 regelt das Verfahren und die Modalitäten der Bestellung des Landesbeauftragten für den Datenschutz und dessen Stellvertreter sowie die Dauer und Beendigung des Amtsverhältnisses des Landesbeauftragten. Die Bestimmung setzt dabei die Vorgaben der Artikel 53 Abs. 1, 3 und 4, Artikel 54 Abs. 1 der Verordnung (EU) 2016/679 sowie Artikel 43 Abs. 1, 2 und 3, Artikel 44 Abs. 1 der Richtlinie (EU) 2016/680 um.

Zu Absatz 1:

Absatz 1 regelt das Verfahren der Wahl und Bestellung des Thüringer Landesbeauftragten für den Datenschutz. Sowohl die Verordnung (EU) 2016/679 als auch die Richtlinie (EU) 2016/680 sehen vor, dass die Mitgliedstaaten der Europäischen Union ein transparentes Verfahren schaffen, durch welches die Mitglieder der Aufsichtsbehörde vom Parlament, von der Landesregierung, vom Staatsoberhaupt oder von einer unabhängigen Stelle ernannt werden. Nach Satz 1 erfolgt die Wahl allein durch den Landtag und ohne Beteiligung der Landesregierung. Satz 2 regelt in Umsetzung von Artikel 54 Abs. 1 Buchst. c der Verordnung (EU) 2016/679 und Artikel 44 Abs. 1 Buchst. c der Richtlinie (EU) 2016/680 das Ernennungsverfahren. Satz 3 bestimmt, dass die Amtszeit mit Aushändigung der Ernennungsurkunde beginnt.

Zu Absatz 2:

Mit Absatz 2 werden in Durchführung der Artikel 53 Abs. 2, 54 Abs. 1 Buchst. b der Verordnung (EU) 2016/679 und in Umsetzung der gleichlautenden Artikel 43 Abs. 2, 44 Abs. 1 Buchst. b der Richtlinie (EU) 2016/680 die Anforderungen an die Qualifikation und sonstigen Voraussetzungen für die Ernennung des Landesbeauftragten für den Datenschutz geregelt.

Zu Absatz 3:

Mit Absatz 3 wird die bisherige Regelung unverändert übernommen. Die Ausgestaltung des öffentlich-rechtlichen Amtsverhältnisses in §§ 3 und 4 sichert die Unabhängigkeit des Landesbeauftragten für den Datenschutz.

Zu Absatz 4:

Absatz 4 regelt die Amtszeit und die Wiederwahl des Landesbeauftragten für den Datenschutz.

Die Amtszeit beträgt sechs Jahre. Sie geht über eine Legislaturperiode des Thüringer Landtags hinaus und stärkt damit seine Unabhängigkeit. Die Möglichkeit der Wiederwahl entsprechend der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 ist begrenzt, da es sich bei dem Datenschutz um ein äußerst dynamisches Rechtsgebiet mit sich ständig wandelnden technischen Herausforderungen handelt. Nach maximal zwölfjähriger Amtszeit ist daher ein personeller Wechsel angezeigt. Zugleich soll die grundsätzliche Möglichkeit der Wiederwahl die Unabhängigkeit stärken.

Zu Absatz 5:

Durch Absatz 5 wird die Bestimmung aus § 35 Abs. 3 ThürDSG a. F. unverändert übernommen. Es handelt sich um eine Konkretisierung des Ernennungsverfahrens.

Zu Absatz 6:

Absatz 6 übernimmt die bisherige Regelung des § 35 Abs. 4 ThürDSG a. F. Das Vorschlagsrecht des Landesbeauftragten für den Datenschutz

ergibt sich aus dem Vertrauensverhältnis, welches zwischen ihm und seinem Stellvertreter erforderlich ist. Die notwendige Sachkunde des Vertreters wird durch die geforderte Befähigung zum Richteramt erreicht.

Zu Absatz 7:

Absatz 7 übernimmt die bisherige Bestimmung des § 35 Abs. 5 ThürDSG a. F.

Zu Absatz 8:

Absatz 8 bestimmt die Voraussetzungen, unter denen das Amtsverhältnis des Landesbeauftragten für den Datenschutz endet oder er entlassen werden kann.

Nach Satz 1 endet das Amt des Landesbeauftragten mit Ablauf der Amtszeit oder mit seinem Rücktritt. Satz 2 regelt die Amtsenthebung durch den Präsidenten des Landtags. Der Begriff der "schweren Verfehlung" wurde unmittelbar dem Artikel 53 Abs. 4 der Verordnung (EU) 2016/679 entnommen. Es handelt sich dabei um einen Begriff des Unionsrechts, der an ein schweres, in der Person liegendes Defizit anknüpft. Im Zuge der Anpassung an die Verordnung (EU) 2016/679 wurde zugleich der Verweis auf die Gründe, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen können, gestrichen. Durch die Anpassung soll aber keinesfalls der Maßstab, der für Richter gilt, unterschritten werden. Bei der Beurteilung der schweren Verfehlung ist die völlige Unabhängigkeit des Landesbeauftragten zu berücksichtigen.

Die Durchsetzung der Amtsenthebung durch den Präsidenten des Landtags stellt eine Konkretisierung des Verfahrens dar. Damit wird auch zum Ausdruck gebracht, dass die Aufsichtsbehörde jeglichem Einfluss durch die Landesregierung entzogen ist.

Zu Absatz 9:

Absatz 9 enthält eine Stellvertreterregelung für den Fall, dass bei Ablauf der Amtszeit des Landesbeauftragten für den Datenschutz ein Nachfolger noch nicht feststeht. Die Stelle der Leitung der Aufsichtsbehörde soll nicht unbesetzt sein. Nach Absatz 9 führt der Landesbeauftragte nach Ablauf der Amtszeit die Geschäfte nur übergangsweise. Damit verbunden sind laufende Geschäfte, keine grundlegenden Entscheidungen. Die Pflicht zur Weiterführung des Amtes gilt jedoch maximal für die Dauer von sechs Monaten. Die Bestimmung entspricht der Regelung auf Bundesebene und bietet dem ausscheidenden Amtswalter eine persönliche Perspektive und Planungssicherheit. Zusätzlich wird sichergestellt, dass insbesondere die Regelungen zur Entlassung auch während des Übergangszeitraumes von sechs Monaten Anwendung finden.

Zu § 4

Rechtsstellung und Verschwiegenheitspflicht des Landesbeauftragten für den Datenschutz (Artikel 51 bis 54 der Verordnung (EU) 2016/679, Artikel 41 bis 44 der Richtlinie (EU) 2016/680)

§ 4 regelt die Rechtsstellung des Landesbeauftragten für den Datenschutz, seine Rechte und Pflichten während und nach der Amtszeit, die Stellung und Aufgaben gegenüber seinem Personal, seine Ausstattung sowie seine haushälterische Stellung.

Die in § 36 Abs. 1 ThürDSG a. F. normierte Unabhängigkeit des Landesbeauftragten ergibt sich nunmehr unmittelbar aus Artikel 52 der Verordnung (EU) 2016/679, was durch den Klammerverweis deutlich gemacht wird und zugleich auch der Umsetzung von Artikel 41 der Richtlinie (EU) 2016/680 dient. Die Dienstaufsicht nach bisherigem Recht wurde gestrichen, um die Unabhängigkeit im Sinne der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 zu stärken. Aufgrund der verbindlich

geltenden Regelung zur Amtsenthebung nach Artikel 53 Abs. 4 der Verordnung (EU) 2016/679 verbliebe eine nur noch schwer eingrenzbar "Aufsichtshülle", die europarechtlich aufgrund der Vorgaben des Artikels 52 Abs. 2 der Verordnung (EU) 2016/679 angreifbar wäre. Die mit seiner Unabhängigkeit einhergehende Weisungsfreiheit folgt unmittelbar aus Artikel 52 Abs. 2 der Verordnung (EU) 2016/679 und dient auch der Umsetzung von Artikel 42 Abs. 2 der Richtlinie (EU) 2016/680.

Zu Absatz 1:

Absatz 1 definiert die Aufsichtsbehörde im Sinne von Artikel 51 der Verordnung (EU) 2016/679 und Artikel 41 der Richtlinie (EU) 2016/680. Zwar definiert auch die Verordnung (EU) 2016/679 den Begriff der Aufsichtsbehörde, allerdings bezieht sich dieser auf diejenige Kontrollbehörde, welche für die Überwachung der Verordnung (EU) 2016/679 zuständig ist. Der Begriff kann daher nicht unmittelbar für den Dritten Abschnitt gelten. Dass der Landesbeauftragte Aufsichtsbehörde im Sinne der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 sein kann, folgt aus Artikel 46 Abs. 3 der Richtlinie (EU) 2016/680.

Zu Absatz 2:

Satz 1 wiederholt Artikel 52 Abs. 3 der Verordnung (EU) 2016/679 und setzt damit Artikel 32 Abs. 3 der Richtlinie (EU) 2016/680 um. Im Unterschied zur Bestimmung im Thüringer Datenschutzgesetz a. F. sind ausdrücklich auch unentgeltliche, nicht mit dem Amt zu vereinbarende Tätigkeiten untersagt. Satz 2 entspricht der bisherigen Regelung des § 36 Abs. 2 ThürDSG a. F. und bestimmt ein umfassendes Verbot sämtlicher mit dem Amt nicht zu vereinbarenden Tätigkeiten. Absatz 2 konkretisiert die Vorgaben des Artikels 52 Abs. 3 der Verordnung (EU) 2016/679 bzw. des Artikels 42 Abs. 3 der Richtlinie (EU) 2016/680.

Zu Absatz 3:

Absatz 3 regelt die Verschwiegenheitspflicht des Landesbeauftragten sowie seiner Mitarbeiter. Die Bestimmung übernimmt Artikel 54 Abs. 2 der Verordnung (EU) 2016/679, der zugleich Artikel 44 Abs. 2 der Richtlinie (EU) 2016/680 entspricht. Es handelt sich um eine europarechtskonforme Anpassung der bisherigen Bestimmung.

Zu Absatz 4:

Absatz 4 bestimmt Ausnahmen von der Verschwiegenheitspflicht nach Absatz 3. Die Bestimmung übernimmt die bisherige Regelung des § 36 Abs. 3 Satz 2 ThürDSG a. F. Sie ergänzt Absatz 3 sachgerecht und gewährleistet, dass der Landesbeauftragte für den Datenschutz seine Aufgaben effektiv wahrnehmen kann. Zur Verbesserung des Datenschutzes ist es legitim, Öffentlichkeitsarbeit zu betreiben, um in der öffentlichen Wahrnehmung Präsenz für das Thema zu schaffen. Durch Absatz 4 soll auch diese Tätigkeit des Landesbeauftragten unterstützt werden.

Zu Absatz 5:

Die Bestimmung entspricht der bisherigen Regelung des § 36 Abs. 4 ThürDSG a. F. Satz 1 stellt klar, dass der Thüringer Landesbeauftragte für den Datenschutz für die Entscheidung über die Vorlage von Akten oder anderen in amtlicher Verwahrung befindlichen Schriftstücken nach § 96 Strafprozessordnung (StPO) oberste Dienstbehörde sowie für Entscheidung über Akteneinsicht nach § 99 der Verwaltungsgerichtsordnung (VwGO) zuständige oberste Aufsichtsbehörde ist.

Sätze 2 und 3 stellen klar, dass der Landesbeauftragte in eigener Verantwortung über die Aussagegenehmigung seiner Mitarbeiter und seiner Vorgänger im Amt entscheidet.

Zu Absatz 6:

Absatz 6 regelt die sachliche, personelle und finanzielle Ausstattung des Landesbeauftragten für den Datenschutz. Satz 1 stellt sicher, dass der Landesbeauftragte durch sachliche, personelle und technische Ausstattung seine Aufgabe wirksam wahrnehmen kann. Die Bestimmung entspricht Artikel 52 Abs. 4 der Verordnung (EU) 2016/679 und setzt damit Artikel 42 Abs. 4 der Richtlinie (EU) 2016/680 um.

Satz 1 legt zudem fest, dass der Landesbeauftragte im Einzelplan des Landtags mit einem eigenen Kapitel ausgestattet wird. Verwaltungsangelegenheiten werden weiterhin von der Landtagsverwaltung wahrgenommen. In diesem Sinne ist der Landesbeauftragte auch künftig beim Landtag angesiedelt.

Satz 2 stellt klar, dass der Landesbeauftragte der Kontrolle durch den Rechnungshof untersteht. Dies gilt aber nur, solange und soweit seine Unabhängigkeit dadurch nicht beeinträchtigt wird. Durch die Bestimmung werden die Vorgaben aus Artikel 52 Abs. 6 der Verordnung (EU) 2016/679 bzw. der gleichlautende Artikel 42 Abs. 6 der Richtlinie (EU) 2016/680 umgesetzt. Demnach hat jeder Mitgliedstaat der Europäischen Union sicherzustellen, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt. Wie aus Erwägungsgrund 118 der Verordnung (EU) 2016/679 folgt, bedeutet die Unabhängigkeit der Aufsichtsbehörden nicht, dass sie hinsichtlich ihrer Ausgaben keinem Kontroll- oder Überwachungsmechanismus unterworfen sind. Jedoch findet die Finanzkontrolle ihre Grenzen in der Unabhängigkeit der Datenschutzaufsicht. Die Haushalts- und Wirtschaftsführung des Landesbeauftragten unterliegt der Prüfung des Rechnungshofs daher nur, soweit hierdurch seine Unabhängigkeit nicht beeinträchtigt wird.

Zu Absatz 7:

Absatz 7 regelt das Verhältnis des Landesbeauftragten für den Datenschutz zu seinen Mitarbeitern.

Es werden die Vorgaben des Artikels 52 Abs. 5 der Verordnung (EU) 2016/679 und des wortgleichen Artikels 42 Abs. 5 der Richtlinie (EU) 2016/680 umgesetzt.

Durch sein Beteiligungsrecht wird die wirksame Arbeit des Landesbeauftragten sichergestellt. Die durch die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680 vorgeschriebene Unabhängigkeit der Aufsichtsbehörde verlangt nicht, dass der Landesbeauftragte organisationsrechtlich eigenen Behördencharakter erhält. Die Prüfung des Vorliegens der beamtenrechtlichen Bestimmungen bei seinen Mitarbeitern und deren Ernennung obliegt daher im Sinne von Artikel 69 der Verfassung des Freistaats Thüringen der Landtagsverwaltung, die weiterhin die Verwaltungsangelegenheiten des Landesbeauftragten wahrnimmt.

Satz 2 übernimmt die bisherige Regelung des § 36 Abs. 6 Satz 2 ThürDSG a. F. und sichert die sachliche Unabhängigkeit der Mitarbeiter, indem sie nur der Weisung des Landesbeauftragten unterworfen sind.

Zu § 5

Anwendung beamtenrechtlicher Vorschriften auf den Landesbeauftragten für den Datenschutz

§ 5 entspricht der bisherigen Bestimmung des § 36 a ThürDSG a. F. Der Landesbeauftragte für den Datenschutz ist zwar kein Landesbeamter, sondern steht zur Wahrung der Unabhängigkeit in einem besonderen öffentlich-rechtlichen Amtsverhältnis, jedoch können die entsprechenden Bestimmungen des Landesbeamtenrechts ergänzend angewandt werden. Die Klarstellung in Absatz 3 Satz 1 ist zur Verhinderung von möglichen Doppelzahlungen ("im Fall des § 3 Abs. 9 nach Ablauf des Tages,

an dem die Geschäftsführung endet") erforderlich, da ansonsten bei wörtlicher Auslegung in dem Zeitraum sowohl Besoldung wie Versorgung zustehen könnten (siehe § 3 Abs. 8, 9 - der Zeitraum ist nicht Teil des Amtsverhältnisses). Absatz 3 Satz 2 soll eine besoldungsrechtliche Gleichstellung mit dem Bürgerbeauftragten (vgl. § 10 Abs. 3 S. 2 Thür-BüBG) bzw. den Thüringer Ministern (vgl. § 11 Abs. 1 S. 2 ThürMinG) herbeiführen. Die Notwendigkeit für eine versorgungsrechtliche Besserstellung gegenüber diesen Amtsverhältnissen besteht nicht.

Zu § 6

Aufgaben des Landesbeauftragten für den Datenschutz (Artikel 57 und 31 der Verordnung (EU) 2016/679, Artikel 46 und 26 der Richtlinie (EU) 2016/680)

§ 6 bestimmt, nach welchen Vorschriften sich die Aufgaben des Thüringer Landesbeauftragten für den Datenschutz im Anwendungsbereich der Verordnung (EU) 2016/679, der entsprechenden Anwendung der Verordnung (EU) 2016/679 und dieses Gesetzes bemessen (Absatz 1), beziehungsweise welche Aufgaben die Aufsichtsbehörde im Anwendungsbereich der Richtlinie (EU) 2016/680 hat.

Zu Absatz 1:

Absatz 1 regelt die Aufgaben des Thüringer Landesbeauftragten für den Datenschutz als Aufsichtsbehörde nach Artikel 51 der Verordnung (EU) 2016/679. Es handelt sich dabei um Datenverarbeitungen

- im Anwendungsbereich der Verordnung (EU) 2016/679 nach § 1 Abs. 1,
- außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 (siehe § 2 Abs. 5) und
- im Anwendungsbereich von in Ergänzung der Verordnung (EU) 2016/679 getroffenen Regelungen.

Dazu stehen ihm die Aufgaben nach Artikel 57 der Verordnung (EU) 2016/679 zu. Dabei kontrolliert der Landesbeauftragte die Einhaltung der Bestimmungen der Verordnung (EU) 2016/679, dieses Gesetzes und anderer datenschutzrechtlicher Bestimmungen.

Zu Absatz 2:

Absatz 2 regelt die Aufgaben des Landesbeauftragten für den Datenschutz zum Zwecke der Umsetzung des Artikels 46 der Richtlinie (EU) 2016/680.

Zu Absatz 3:

Durch Absatz 3 werden Artikel 31 der Verordnung (EU) 2016/679 und Artikel 26 der Richtlinie (EU) 2016/680 umgesetzt.

Zu § 7

Befugnisse des Landesbeauftragten für den Datenschutz (Artikel 58 und 83 der Verordnung (EU) 2016/679, Artikel 47 der Richtlinie (EU) 2016/680)

§ 7 regelt, welche Befugnisse der Aufsichtsbehörde zur Erfüllung ihrer Aufgaben nach § 6 zur Seite stehen.

Zu Absatz 1:

Im Anwendungsbereich der Verordnung ergeben sich die Befugnisse aus Artikel 58 der Verordnung (EU) 2016/679. Es handelt sich dabei um Untersuchungsbefugnisse (Absatz 1), Abhilfebefugnisse (Absatz 2) und Genehmigungsbefugnisse (Absatz 3). Dabei beziehen sich die Befugnisse nicht nur auf Verstöße gegen die Verordnung (EU) 2016/679,

sondern auch auf Verstöße gegen dieses Gesetz und andere datenschutzrechtliche Bestimmungen. Durch die Sätze 2 bis 5 wird dem Landesbeauftragten aufgegeben, vor Ergreifen der Maßnahmen nach Artikel 58 Abs. 2 der Verordnung (EU) 2016/679 den Verantwortlichen und die Aufsichtsbehörde anzuhören. Durch die Sätze 2 bis 5 wird das ehemalige Beanstandungsrecht, welches in Artikel 58 der Verordnung (EU) 2016/679 nicht namentlich vorgesehen ist, soweit aufrecht erhalten, wie sich die damit verbundenen Befugnisse nicht unmittelbar aus Artikel 58 Abs. 1 Buchst. d und Abs. 2 der Verordnung (EU) 2016/679 ergeben.

Zu Absatz 2:

Durch Satz 1 wird von der Möglichkeit Gebrauch gemacht, das Zugangsrecht der Aufsichtsbehörde zu Geschäftsräumen nach Artikel 58 Abs. 1 Buchst. f der Verordnung (EU) 2016/679 zu konkretisieren.

Satz 2 bestimmt, dass gegen öffentliche Stellen keine Geldbußen verhängt werden dürfen, es sei denn, diese nehmen am Wettbewerb teil. Nach Artikel 83 Abs. 1 der Verordnung (EU) 2016/679 steht den Aufsichtsbehörden die Befugnis zur Verhängung von Geldbußen nach Artikel 83 Abs. 2 bis 6 der Verordnung (EU) 2016/679 zu. Nach Artikel 83 Abs. 7 der Verordnung (EU) 2016/679 können Mitgliedstaaten der Europäischen Union allerdings durch Vorschriften bestimmen, dass gegen öffentliche Stellen diese Befugnis nicht besteht. Davon macht Satz 2 Gebrauch. Sanktionen in der von Artikel 83 der Verordnung (EU) 2016/679 vorgesehenen Form und Höhe sind in dem öffentlichen Bereich weder erforderlich noch angemessen und dem deutschen Verfassungsrecht fremd. Bei Verstößen gegen die in Artikel 83 Abs. 1 bis 6 der Verordnung (EU) 2016/679 genannten Bestimmungen sind vielmehr die Rechtsaufsichtsbehörden zum Handeln aufgerufen.

Zu Absatz 3:

Personenbezogene Daten, die einem Berufsgeheimnis unterliegen, unterstehen der Kontrolle durch den Landesbeauftragten für den Datenschutz. Dies entspricht insoweit der bisherigen Bestimmung in § 37 Abs. 2 ThürDSG a. F. Die ausdrückliche Erwähnung der Kontrolle bei Akten, die einem besonderen Amtsgeheimnis unterliegen, ist entfallen, da die Verordnung (EU) 2016/679 nicht zwischen Berufs- und besonderem Amtsgeheimnis unterscheidet. Darüber hinaus hat sich der Begriff in der Anwendung als zu unspezifisch erwiesen.

Für personenbezogene Daten in Akten über Sicherheitsüberprüfungen gilt das Kontrollrecht nur, wenn die betroffene Person nicht widersprochen hat. Es handelt sich in der Regel dort um besonders sensible Daten und das informationelle Selbstbestimmungsrecht der betroffenen Person bedarf somit eines besonderen Schutzes. Der Verantwortliche hat die betroffene Person auf ein ihr zustehendes Widerspruchsrecht hinzuweisen. Es handelt sich bei Akten über Sicherheitsüberprüfung um Sachverhalte außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679, so dass eine spezielle Regelung zulässig ist.

Zu Absatz 4:

Absatz 4 bestimmt, in welchen Fällen der Landesbeauftragte für den Datenschutz kein Recht zur Kontrolle hat. Die Bestimmung entspricht der bisherigen Regelung des § 37 Abs. 3 ThürDSG a. F. Daten, die der Kontrolle durch die Kommission nach § 3 des Thüringer Gesetzes zur Ausführung des Artikel 10-Gesetzes unterliegen, fallen nicht in den Anwendungsbereich der Verordnung (EU) 2016/679. Eine spezielle Ausnahmeregelung ist daher zulässig. Diese Daten bedürfen wegen der bereits vorliegenden Kontrolle in der Regel keiner weiteren Kontrolle durch den Landesbeauftragten. Die Kommission hat aber stets die Möglich-

keit, sich der Expertise des Landesbeauftragten durch Ersuchen an ihn zu bedienen. Eine Verpflichtung des Landesbeauftragten ist damit jedoch nicht verbunden, sie wäre mit der abschließenden Aufzählung der Aufgaben in Artikel 57 der Verordnung (EU) 2016/679 nicht vereinbar.

Zu Absatz 5:

Absatz 5 ergänzt das Sicherheitsbedürfnis der in § 21 Abs. 3 genannten Stellen um die Unterstützungspflicht dieser Stellen ausschließlich gegenüber dem Landesbeauftragten für den Datenschutz selbst und der von ihm schriftlich Beauftragten.

Die Regelungsbefugnis für Absatz 4 folgt aus dem Umstand, dass Sicherheitsbehörden nicht dem Anwendungsbereich der Verordnung (EU) 2016/679 (Artikel 2 Abs. 2 der Verordnung (EU) 2016/679) und damit nach § 1 Abs. 1 auch nicht dem Zweiten Abschnitt unterfallen.

Zu Absatz 6:

Absatz 6 regelt das Beanstandungsrecht des Landesbeauftragten für den Datenschutz sowie das Recht zur Warnung.

Die bisherige Bestimmung des § 39 ThürDSG a. F. wird übernommen und ergänzt durch die beispielhaft aufgeführten Elemente des Artikels 47 Abs. 2 der Richtlinie (EU) 2016/680. Das Beanstandungsrecht gilt nicht für Datenverarbeitungen im Anwendungsbereich der Verordnung (EU) 2016/679. Dort geht das Beanstandungsrecht bereits in den Befugnissen nach Artikel 58 der Verordnung (EU) 2016/679 auf.

Das Recht zur Beanstandung gilt folglich nur im Rahmen der Datenverarbeitung nach § 31 sowie für Datenverarbeitungen, die weder der Verordnung (EU) 2016/679 noch § 31 unterfallen.

Im Rahmen der Datenverarbeitung nach § 31 des Gesetzes richten sich die Befugnisse des Landesbeauftragten für den Datenschutz nach Artikel 47 der Richtlinie (EU) 2016/680. Dem Landesbeauftragten werden nach der Regelungssystematik in dieser Bestimmung keine Durchgriffsbefugnisse gegenüber Verantwortlichen gegeben, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständig sind - wobei die Verfolgung von Straftaten den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit umfasst - und soweit sie zu diesen Zwecken Daten verarbeiten. Dies folgt aus der unterschiedlichen Ausgestaltung der Abhilfebefugnisse in der Verordnung (EU) 2016/679 einerseits und der Richtlinie (EU) 2016/680 und den dort bestehenden fachlichen Bedürfnissen andererseits, weshalb die Richtlinie mehr Flexibilität eröffnet. Im Bereich der Straftatenverhütung, -ermittlung und -verfolgung sowie der darauf bezogenen Gefahrenabwehr lassen sich Letztentscheidungs- und Anordnungsbefugnisse des Landesbeauftragten (vergleichbar mit Artikel 58 der Verordnung (EU) 2016/679) nicht mit der Sensibilität und Komplexität der entsprechenden Verarbeitungen und dem Bedürfnis nach ständiger Verfügbarkeit rechtmäßig erhobener Daten und Datenverarbeitungsanlagen in Einklang bringen. Die Einräumung von Durchgriffsbefugnissen in spezialgesetzlichen Regelungen bleibt davon unberührt.

Dies gilt entsprechend für den nicht EU-rechtlich erfassten Bereich von Verarbeitungen zu Zwecken außerhalb beider Rechtsakte. Absatz 6 stellt eine von der Verordnung (EU) 2016/679 abweichende Regelung für diese Datenverarbeitungen dar, da Artikel 58 der Verordnung (EU) 2016/679 keine Anwendung findet.

Zu § 8**Anrufung des Landesbeauftragten für den Datenschutz (Artikel 77 der Verordnung (EU) 2016/679 , Artikel 52 der Richtlinie (EU) 2016/680)**

Durch die Bestimmung werden entsprechende Vorgaben der Richtlinie (EU) 2016/680 umgesetzt, die den Regelungen der Verordnung (EU) 2016/679 entsprechen. Es handelt sich bei dem Beschwerderecht gegenüber dem Landesbeauftragten für den Datenschutz, wenn datenschutzrechtliche Verstöße zu vermuten sind, um eine seiner wesentlichen Funktionen.

Zu Absatz 1:

§ 8 stellt klar, dass sich betroffene Personen mit Beschwerden über die bei Verantwortlichen durchgeführte Verarbeitung an den Landesbeauftragten für den Datenschutz wenden können. Insbesondere mit Absatz 1 dieser Bestimmung werden gleichzeitig Artikel 77 der Verordnung (EU) 2016/679 und Artikel 52 der Richtlinie (EU) 2016/680 umgesetzt. Absatz 1 entspricht weitestgehend der bisherigen Regelung des § 11 ThürDSG a. F. Durch Satz 2 werden die Vorgaben aus Artikel 77 Abs. 2 der Verordnung (EU) 2016/679 und aus Artikel 52 Abs. 4 der Richtlinie (EU) 2016/680 umgesetzt.

Zu Absatz 2:

Absatz 2 übernimmt das Verbot der Benachteiligung und Maßregelung gegenüber der betroffenen Person, wenn diese sich an den Landesbeauftragten für den Datenschutz wendet.

Zu Absatz 3:

Absatz 3 entspricht der bisherigen Regelung in § 11 Abs. 3 ThürDSG a. F. und ergänzt § 21 Abs. 5.

Zu Absatz 4:

Absatz 4 setzt Artikel 77 Abs. 2 der Verordnung (EU) 2016/679 sowie Artikel 52 Abs. 2 und 3 der Richtlinie (EU) 2016/680 um.

Zu § 9**Rechtsschutz gegen Anordnungen des Landesbeauftragten für den Datenschutz oder bei dessen Untätigkeit (Artikel 78 der Verordnung (EU) 2016/679, Artikel 53 der Richtlinie (EU) 2016/680)****Zu Absatz 1:**

§ 9 setzt Artikel 78 Abs. 1 der Verordnung (EU) 2016/679 und Artikel 53 der Richtlinie (EU) 2016/680 um und bestimmt, dass öffentliche Stellen, welche Adressaten von verbindlichen Beschlüssen des Landesbeauftragten für den Datenschutz sind, Rechtsschutz dagegen ersuchen können.

Zu Satz 1:

Der Rechtsschutz besteht gegen rechtsverbindliche Beschlüsse des Landesbeauftragten im Sinne von Artikel 78 Abs. 1 der Verordnung (EU) 2016/679 und § 7 Abs. 6 ThürDSG in Umsetzung von Artikel 53 der Richtlinie (EU) 2016/680. In Erwägungsgrund 143 der Verordnung (EU) 2016/679 und in Erwägungsgrund 86 der Richtlinie (EU) 2016/680 wird betont, dass sich der Rechtsschutz insbesondere auf die Ausübung von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen oder die Ablehnung oder Abweisung von Beschwerden durch die Aufsichtsbehörde bezieht; für reine Stellungnahmen oder Empfehlungen hingegen soll der Anwendungsbereich nicht eröffnet sein.

Von der Bestimmung nicht erfasst ist der Rechtsschutz gegen die Verhängung von Ordnungswidrigkeiten nach § 61.

Zu Satz 2:

Satz 2 verweist auf die Bestimmungen des § 20 Abs. 2 bis 7 BDSG in der Fassung vom 30. Juni 2017 (BGBl. I S. 2097) in der jeweils geltenden Fassung, die mit der Maßgabe, dass "Aufsichtsbehörde" der Landesbeauftragte für den Datenschutz ist, entsprechend anwendbar sind. § 20 Abs. 2 bis 7 bestimmen, dass der Verwaltungsrechtsweg eröffnet ist (Absatz 2), die örtliche Zuständigkeit (Absatz 3), die Beteiligungsfähigkeit nach § 61 VwGO (Absatz 4), die Beteiligten des Verfahrens nach § 63 VwGO (Absatz 5), den Ausschluss des Vorverfahrens (Absatz 6) sowie der sofortigen Vollziehung nach § 80 Abs. 2 Satz 1 Nr. 4 VwGO (Absatz 7). Das Vorverfahren wird mangels Devolutiveffekts ohne einer dem Landesbeauftragten übergeordneten Behörde ausgeschlossen. Der Landesbeauftragte ist nicht befugt, durch Verwaltungsentscheidung die aufschiebende Wirkung der Anfechtungsklage einer öffentlichen Stelle auszuschließen. Unbeschadet der Anordnungscompetenz des Landesbeauftragten für den Datenschutz stehen sich die beteiligten Verwaltungsträger nicht in einem Subordinationsverhältnis gegenüber. Im Falle einer Verwaltungsstreitsache kann eine verbindliche Entscheidung allein durch das Verwaltungsgericht getroffen werden.

Sofern die Datenverarbeitung in den Anwendungsbereich des Bundesdatenschutzgesetzes fällt, ist § 20 BDSG unmittelbar anwendbar.

Dass der Landesbeauftragte für Datenschutz zur Durchsetzung der Befugnisse nach Artikel 58 der Verordnung (EU) 2016/679 gegenüber juristischen Personen des öffentlichen Rechts und Behörden keine Zwangsmaßnahmen ausüben darf, ergibt sich bereits aus dem Umstand, dass es an einer entsprechenden Ermächtigung durch Gesetz oder aufgrund eines Gesetzes nach den Vorgaben des § 44 Abs. 3 Thüringer Verwaltungszustellungs- und Vollstreckungsgesetz (ThürVwZVG) fehlt.

Zu Absatz 2:

In Absatz 2 wird - in Umsetzung von Artikel 78 Abs. 2 der Verordnung (EU) 2016/679 und Artikel 53 Abs. 2 der Richtlinie (EU) 2016/680 - der Rechtsschutz auf Fälle der Untätigkeit des Landesbeauftragten für den Datenschutz ausgedehnt.

Zu § 10

Weitere Aufgaben des Landesbeauftragten für den Datenschutz (Artikel 59 der Verordnung (EU) 2016/679, Artikel 49 der Richtlinie (EU) 2016/680)

§ 10 regelt verfahrensrechtliche Einzelheiten zum Tätigkeitsbericht des Landesbeauftragten für den Datenschutz nach Artikel 59 der Verordnung (EU) 2016/679 und des inhaltsgleichen Artikels 49 der Richtlinie (EU) 2016/680. Des Weiteren regelt Absatz 4 der Bestimmung weitere Rechte des Landtags und der Landesregierung gegenüber dem Landesbeauftragten.

Zu Absatz 1:

Die Pflicht der Aufsichtsbehörde, jährlich einen Tätigkeitsbericht zu erstellen und diesen zugänglich zu machen, ergibt sich aus Artikel 59 der Verordnung (EU) 2016/679 unmittelbar, durch Absatz 1 wird die gleichlautende Bestimmung des Artikels 49 der Richtlinie (EU) 2016/680 umgesetzt.

Eine Regelung zum Tätigkeitsbericht im nichtöffentlichen Bereich findet sich in § 11 Abs. 2.

Zu Absatz 2:

Absatz 2 enthält spezifische Bestimmungen zum Tätigkeitsbericht. Die Verordnung (EU) 2016/679 enthält zwar keine Pflicht zur Stellungnahme, gleichwohl soll an dem bisherigen Verfahren und der Diskussion des Berichts im Landtag festgehalten werden.

Die Bestimmung legt daher fest, dass der Ministerpräsident eine Stellungnahme der Landesregierung zum Tätigkeitsbericht herbeiführt, die binnen vier Monaten dem Landtag vorzulegen ist. Der Tätigkeitsbericht ist ein bedeutsames Mittel zur Verbesserung des Datenschutzes und soll die Lage des Datenschutzes in den öffentlichen Stellen beschreiben. Durch die Berichterstattung gegenüber dem Landtag und der Landesregierung soll die Tätigkeit eine entsprechende Resonanz in der Öffentlichkeit erlangen.

Dies entspricht zum Teil der bisherigen Regelung des § 40 Abs. 1 Satz 3 ThürDSG a. F. Es handelt sich um eine spezifische Bestimmung, der Artikel 6 Abs. 1 Buchst. e und Abs. 3 der Verordnung (EU) 2016/679 zugrunde liegt. Die Bestimmung bezieht sich nur auf den Tätigkeitsbericht im öffentlichen Bereich.

Zu Absatz 3:

Der Bericht ist im Beirat nach § 12 vorzubereiten. Es handelt sich um eine spezifische Bestimmung, der Artikel 6 Abs. 1 Buchst. e und Abs. 3 der Verordnung (EU) 2016/679 zugrunde liegt und um eine Konkretisierung der Richtlinie (EU) 2016/680. Die Vorberatung beeinträchtigt ausdrücklich nicht die Unabhängigkeit des Landesbeauftragten für den Datenschutz, so auch die Begründung zu § 12.

Zu Absatz 4:

Es handelt sich bei den in Absatz 4 genannten Aufgaben um Konkretisierungen im Rahmen von Artikel 57 Abs. 1 der Verordnung (EU) 2016/679 und von Artikel 46 der Richtlinie (EU) 2016/680. Insbesondere Artikel 57 Abs. 1 Buchst. c der Verordnung (EU) 2016/679 und Artikel 46 Abs. 1 Buchst. c der Richtlinie (EU) 2016/680 formulieren an die Mitgliedstaaten der Europäischen Union den Handlungsauftrag, eine Rechtsgrundlage für die Beratung nationaler Parlamente, Regierungen und anderer Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen durch die Aufsichtsbehörde zu schaffen. An dieser Stelle steht es den Mitgliedstaaten daher frei, zusätzliche Regelungen zu treffen. Dies greift die Bestimmung auf.

Landesregierung und Landtag können den Landesbeauftragten für den Datenschutz um Gutachten und Berichte sowie um Prüfung bestimmter Vorgänge aus ihrem Aufgabenbereich ersuchen. Eine Verpflichtung durch Landesregierung oder Landtag - wie im bisherigen Recht vorgesehen - wäre mit der Unabhängigkeit des Landesbeauftragten sowie mit der abschließenden Aufzählung der Aufgaben in Artikel 57 der Verordnung (EU) 2016/679 nicht vereinbar.

Zu § 11

Aufsichtsbehörde gegenüber nichtöffentlichen Stellen und öffentlichen Stellen, die am Wettbewerb teilnehmen

Der Thüringer Landesbeauftragte für den Datenschutz ist auch die zuständige Aufsichtsbehörde für nichtöffentliche Stellen sowie für öffentliche Stellen, die am Wettbewerb teilnehmen.

Die Regelung ergänzt § 40 Abs. 1 BDSG. Die entsprechenden Aufgaben und Befugnisse des Thüringer Landesbeauftragten regelt § 40 BDSG abschließend.

Absatz 2 ergänzt die Bestimmung zum Tätigkeitsbericht für den nicht-öffentlichen Bereich.

Zu § 12 Beirat

§ 12 entspricht weitestgehend der bisherigen Regelung des § 41 ThürDSG a. F. Der Landesbeauftragte für den Datenschutz wird durch einen Beirat in seiner Arbeit unterstützt. Vorrangig besteht diese Unterstützung darin, den Landesbeauftragten zu beraten. Dadurch sollen weder die Unabhängigkeit des Landesbeauftragten noch ihm seine nach der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 zugewiesenen Aufgaben beeinträchtigt werden. Dem Datenschutz wird dadurch zusätzliches Gewicht und Durchsetzungsvermögen verliehen. Diese Intention ist auch mit den Zwecken der Verordnung (EU) 2016/679 (Artikel 52 und Erwägungsgrund 118) und der Richtlinie (EU) 2016/680 (Artikel 21 und Erwägungsgrund 78) vereinbar.

Zu Absatz 1 bis 4:

Absatz 1 verdeutlicht durch die Zusammensetzung des Beirats die Vielfalt und Beteiligung aller politischen Kräfte auf Landesebene: die im Landtag vertretenen politischen Parteien, Landesregierung, kommunale Spitzenverbände und gesetzliche Sozialversicherungsträger.

Die Mitglieder des Beirats werden nach Absatz 2 grundsätzlich für vier Jahre, die in ihm vertretenen Mitglieder des Landtags für die Wahldauer des Landtags bestellt. Eine wiederholte Bestellung einzelner Mitglieder ist zulässig.

Absatz 3 regelt das Verhältnis von Beirat und Landesbeauftragten für den Datenschutz. Aufgabe des Beirats ist die Unterstützung des Landesbeauftragten. Die Mitglieder des Beirats werden nicht als Kontrolleure des Landesbeauftragten, sondern als Repräsentanten sowohl des politischen als auch behördlichen Sachverständs sowie kommunaler Belange eingebunden. Der Beirat dient damit der wechselseitigen Kommunikation der Institutionen des Freistaats Thüringen in datenschutzrechtlichen Belangen.

Der Beirat gibt sich nach Absatz 4 eine eigene Geschäftsordnung, die das Nähere regelt.

Jedes Mitglied des Beirats hat das Recht, diesen einzuberufen. Für den Landesbeauftragten gilt dies entsprechend. Den Vorsitz im Beirat führt stets ein Beiratsmitglied des Landtags. Der Beirat ist allerdings kein parlamentarisches Kontrollgremium und auch kein Organ des Landtags.

Zu Absatz 5:

Der Landesbeauftragte für den Datenschutz hat ein Teilnahmerecht an allen Sitzungen des Beirats. Im Unterschied zur Regelung nach bisherigem Recht ist der Landesbeauftragte nicht mehr verpflichtet, an allen Sitzungen teilzunehmen. Eine verbindliche Pflicht wäre mit den vorgegebenen Aufgaben und Befugnissen nach Artikel 57 und Artikel 58 der Verordnung (EU) 2016/679 beziehungsweise Artikel 46 und Artikel 47 der Richtlinie (EU) 2016/680 unvereinbar. Aufgrund seiner Unterstützungsfunktion gegenüber dem Landesbeauftragten ist aber eine Teilnahme des Landesbeauftragten an den Sitzungen des Beirats grundsätzlich wünschenswert. Nach dem neu eingefügten Satz 2 hat daher der Vorsitzende des Beirats den Landesbeauftragten so rechtzeitig einzuladen und ihm die Tagesordnung mitzuteilen, dass dieser ein Erscheinen ermöglichen kann. Ebenso ist es zu begrüßen, wenn der Landesbeauftragte den Beirat von seinen wesentlichen Entscheidungen unterrichtet

und möglichst frühzeitig über bedeutsame Entwicklungen auf dem Gebiet des Datenschutzes informiert.

Dem Beirat kann nach Satz 3 Gelegenheit zur Stellungnahme durch den Landesbeauftragten gegeben werden.

Die bisherige Regelung über eine Unterrichtungspflicht beim Gebrauchmachen von bestimmten Befugnissen gegenüber dem Beirat wird aufgehoben. Die Befugnisse des Landesbeauftragten ergeben sich nunmehr unmittelbar aus Artikel 58 der Verordnung (EU) 2016/679 beziehungsweise Artikel 47 der Richtlinie (EU) 2016/680, ergänzt durch § 7.

Der Landesbeauftragte ist an den Inhalt der Stellungnahme des Beirats nicht gebunden.

Zu Absatz 6:

Absatz 6 entspricht der bisherigen Bestimmung des § 41 Abs. 6 ThürDSG a. F. und verpflichtet die Mitglieder des Beirats zur Verschwiegenheit über die ihnen bei ihrer Tätigkeit bekannt gewordenen Angelegenheiten.

Zum Dritten Unterabschnitt Datenschutzbeauftragter

Der Dritte Unterabschnitt ergänzt die Bestimmungen der Artikel 37 bis Artikel 39 der Verordnung (EU) 2016/679 und setzt damit zugleich Artikel 32 bis Artikel 34 der Richtlinie (EU) 2016/680 um. Die Rechtsstellung des Datenschutzbeauftragten in öffentlichen Stellen des Landes wird einheitlich ausgestaltet. Anknüpfungspunkt ist, dass sowohl nach der Verordnung (EU) 2016/679 als auch nach der Richtlinie (EU) 2016/680 Verantwortlicher und Auftragsverarbeiter einen Datenschutzbeauftragten benennen müssen. Dabei sind die Aufgaben des Verantwortlichen durch den jeweiligen Wortlaut der Artikel in der Verordnung (EU) 2016/679 und der Richtlinie 2016/680 eindeutig erkennbar, die Aufgaben des Datenschutzbeauftragten sind in Artikel 39 beziehungsweise in § 15 abschließend geregelt. Die Aufgaben des Verantwortlichen sind zentral in Artikel 5 Abs. 2 und Kapitel 4 der Verordnung (EU) 2016/679 geregelt. Grundsätzlich bleibt daher der Verantwortliche für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich und ist hierfür nachweislichpflichtig.

Zu § 13

Bestellung des Datenschutzbeauftragten (Artikel 37 der Verordnung (EU) 2016/679, Artikel 32 der Richtlinie (EU) 2016/680)

§ 13 regelt die Bestellung eines Datenschutzbeauftragten durch alle öffentlichen Stellen des Landes, sofern sie Daten als Verantwortlicher oder Auftragsverarbeiter verarbeiten. § 13 setzt dabei Artikel 37 der Verordnung (EU) 2016/679 und damit zugleich Artikel 32 der Richtlinie (EU) 2016/680 um.

Zu Absatz 1:

Artikel 37 Abs. 4 und Abs. 1 der Verordnung (EU) 2016/679 sehen vor, dass öffentliche Stellen in jedem Fall einen Datenschutzbeauftragten bestellen müssen, wenn dies gesetzlich vorgeschrieben ist. Hiervon macht Absatz 1 Gebrauch und setzt damit zugleich Artikel 32 Abs. 1 der Richtlinie (EU) 2016/680 um.

Zu Absatz 2:

Neben dem Datenschutzbeauftragten kann jede öffentliche Stelle weitere Vertreter bestellen, wenn sie dies für erforderlich und durchführbar hält. Das Erfordernis mehrerer Vertreter kann insbesondere im Falle der Bestellung eines Datenschutzbeauftragten für mehrere öffentliche

Stellen bestehen. Die Möglichkeit zur Bestellung weiterer Vertreter folgt aus der Aufgabe, die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680 in der Praxis durchzuführen (vergleiche Aufgaben des Datenschutzbeauftragten nach Artikel 39 der Verordnung (EU) 2016/679, Artikel 34 der Richtlinie (EU) 2016/680). Dies erfordert die jederzeitige Verfügbarkeit eines Datenschutzbeauftragten. Die Bestellung eines Vertreters stellt daher nicht nur auf eine bereits nach bisheriger Rechtslage bestehende Möglichkeit der Abwesenheitsvertretung ab, sondern auf eine ständige Vertretung. Dies ermöglicht eine Aufgabenteilung, eröffnet die Möglichkeit zur Rücksprache zwischen beiden Personen und stärkt so letztlich den Datenschutz.

In Ausübung der Aufgaben des Datenschutzbeauftragten sind auf den Stellvertreter die §§ 13 Abs. 3 bis 6 sowie die §§ 14 und 15 in Gänze anwendbar.

Zu Absatz 3:

Regelungen zur Dauer der Bestellung und die Möglichkeit der Wiederbestellung gemäß der bisherigen Bestimmung in § 10 a Abs. 1 Satz 2 ThürDSG a. F. sind in der Verordnung nicht vorgesehen. Die Regelungsbefugnis ergibt sich aber aus Artikel 6 Abs. 1 Buchst. e in Verbindung mit Artikel 6 Abs. 2 der Verordnung (EU) 2016/679. Es handelt sich bei der Regelung um eine spezifische Bestimmung, die der Verarbeitung nach Treu und Glauben dient. Die Verarbeitung nach Treu und Glauben betrifft die Art und Weise der Rechtsausübung im Verhältnis zwischen dem Verantwortlichen und der betroffenen Person. Wie die englische Übersetzung andeutet, zielt der europarechtlich geprägte Begriff auf die Gewährleistung einer fairen Verarbeitung ab. Er verbietet eine unzulässige Rechtsausübung gegenüber der betroffenen Person durch den Verantwortlichen oder Auftragsverarbeiter. Ohne eine Regelung zur Bestelldauer und Wiederbestellung besteht Rechtsunsicherheit für den Datenschutzbeauftragten und auch die betroffenen Personen, denen er zu Rate stehen soll (Artikel 38 Abs. 4 der Verordnung (EU) 2016/679). Die Bestelldauer und Möglichkeit der Wiederbestellung sollen die Position des Datenschutzbeauftragten stärken und flankieren die Regelung des Artikels 38 Abs. 3 Satz 2 der Verordnung (EU) 2016/679.

Zu Absatz 4:

Nach Artikel 37 Abs. 3 der Verordnung (EU) 2016/679 und Artikel 32 Abs. 3 der Richtlinie (EU) 2016/680 kann für mehrere Stellen ein gemeinsamer Datenschutzbeauftragter bestellt werden. Die Bestimmung berücksichtigt, dass in kleinen Organisationseinheiten die Benennung eines Datenschutzbeauftragten mit der erforderlichen Qualifikation problematisch sein kann.

Zu Absatz 5:

Die Bestimmung wiederholt Artikel 37 Abs. 5 der Verordnung (EU) 2016/679 und setzt zugleich Artikel 32 Abs. 2 der Richtlinie (EU) 2016/680 um. Das erforderliche Fachwissen umfasst insbesondere das Datenschutzrecht, erstreckt sich aber auch auf die Datenschutzpraxis. Es kommt damit neben der abstrakten Rechtskenntnis auch auf Umsetzungskenntnis an. Zu den Fähigkeiten, die zur Erfüllung seiner Aufgaben erforderlich sind, zählen Zuverlässigkeit, soziale Kompetenz und Kommunikationsfähigkeit, um seiner Informations- und Beratungsaufgabe gerecht zu werden.

Zu Absatz 6:

Absatz 6 macht Gebrauch von der Möglichkeit, welche die Verordnung (EU) 2016/679 in Artikel 37 Abs. 6 bietet. Der Datenschutzbeauftragte

muss nicht intern gefunden werden, sondern kann auch Externer sein und durch Dienstleistungsvertrag verpflichtet werden. Insbesondere in kleinen Organisationseinheiten, in denen sich ein Datenschutzbeauftragter mit den erforderlichen Qualifikationen unter Umständen schwer finden dürfte, wird so die Möglichkeit eröffnet, den Sachverstand von außen zu holen.

Zu Absatz 7:

Die Bestimmung setzt Artikel 37 Abs. 7 der Verordnung (EU) 2016/679 und Artikel 32 Abs. 4 der Richtlinie (EU) 2016/680 um. Zu den Kontaktdaten zählen die Telefondurchwahl sowie die E-Mail-Adresse des Datenschutzbeauftragten.

Zu § 14

Stellung des Datenschutzbeauftragten (Artikel 38 der Verordnung (EU) 2016/679, Artikel 33 der Richtlinie (EU) 2016/680)

§ 14 regelt die Rechtsstellung des Datenschutzbeauftragten. Die Bestimmung setzt Artikel 38 der Verordnung (EU) 2016/679 und Artikel 33 der Richtlinie (EU) 2016/680 um.

Zu Absatz 1 und 2:

Die Absätze 1 und 2 setzen Artikel 33 der Richtlinie (EU) 2016/680 um. Sie entsprechen Artikel 38 Abs. 1 und 2 der Verordnung (EU) 2016/679.

Zu Absatz 3:

Absatz 3 überträgt die Vorgaben des Artikels 38 Abs. 3 der Verordnung (EU) 2016/679 wortgleich auf alle öffentlichen Stellen des Freistaats, unabhängig davon, zu welchem Zweck die Datenverarbeitung erfolgt. Dies geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus, widerspricht ihr aber nicht.

Das Benachteiligungsverbot in Satz 3 ist umfassend zu verstehen und erfasst jede direkte oder indirekte Diskriminierung oder Sanktionierung des Datenschutzbeauftragten, wenn es sich bei der Maßnahme um eine Reaktion auf seine Positionierung in Angelegenheiten des Datenschutzes handelt.

Zu Absatz 4:

Bei dem besonderen Abberufungs- und Kündigungsschutz des Datenschutzbeauftragten handelt es sich um eine arbeitsrechtliche Regelung, die ergänzend zu den Vorgaben der Verordnung (EU) 2016/679 implementiert werden kann.

Durch Absatz 4 soll die Stellung des Datenschutzbeauftragten gestärkt werden, indem die Möglichkeiten einer Abberufung stark eingeschränkt werden. Eine ordentliche Kündigung des Datenschutzbeauftragten ist aufgrund des sonst jedenfalls für den internen Datenschutzbeauftragten entstehenden Konflikts unzulässig.

Der Datenschutzbeauftragte kann von seinem Amt aus den Gründen des § 626 Bürgerliches Gesetzbuch (BGB) abberufen werden, ohne gekündigt zu werden oder aber ihm kann nach Maßgabe des § 626 BGB gekündigt werden. § 14 Abs. 4 gilt entsprechend für das Vertragsverhältnis des externen Datenschutzbeauftragten. Die Abberufung selbst unterliegt keiner Formvorgabe, im Falle der Beendigung des Arbeitsverhältnisses ist indes auch § 623 BGB zu beachten.

Bestellung und Abberufung des Datenschutzbeauftragten haben sowohl eine datenschutzrechtliche als auch eine arbeitsrechtliche Komponente. Der Verweis auf § 626 BGB ist daher nur unter Berücksichtigung der Stellung des Datenschutzbeauftragten zu lesen. Wichtig sind

diejenigen Gründe, die mit der Funktion des Beauftragten zusammenhängen und die eine weitere Ausübung der Funktion unmöglich machen oder sie gefährden.

Zu Absatz 5:

Absatz 5 überträgt die Vorgaben des Artikels 38 Abs. 4 der Verordnung (EU) 2016/679 wortgleich auf alle öffentlichen Stellen des Freistaats, unabhängig davon, zu welchem Zweck die Datenverarbeitung erfolgt. Dies geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus, widerspricht ihr aber nicht.

Zu Absatz 6:

Die Regelung zur Verschwiegenheitspflicht in Absatz 6 entspricht der bisherigen Bestimmung des § 10 a Abs. 5 ThürDSG a. F. Die Verletzung von Privatgeheimnissen durch den Datenschutzbeauftragten ist nach § 203 Abs. 2a des Strafgesetzbuchs (StGB) zudem strafbewehrt.

Zu Absatz 7:

Absatz 7 überträgt die Vorgaben des Artikels 38 Abs. 6 der Verordnung (EU) 2016/679 wortgleich auf alle öffentlichen Stellen des Freistaats, unabhängig davon, zu welchem Zweck die Datenverarbeitung erfolgt. Dies geht über die Vorgaben der Richtlinie (EU) 2016/680 hinaus, widerspricht ihr aber nicht.

Zu § 15

Aufgaben des Datenschutzbeauftragten (Artikel 39 der Verordnung (EU) 2016/679, Artikel 34 der Richtlinie (EU) 2016/680)

§ 15 regelt die Aufgaben des Datenschutzbeauftragten nach der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680.

Die Gewährleistung des Datenschutzes nach Kapitel IV der Verordnung (EU) 2016/679 sowie Kapitel IV der Richtlinie (EU) 2016/680 obliegt dabei dem Verantwortlichen und dem Auftragsverarbeiter. Sofern also nicht in Artikel 39 der Verordnung (EU) 2016/679 oder in § 15 Abs. 2 originäre Aufgaben des Datenschutzbeauftragten genannt werden, so obliegt ihm lediglich die Unterrichts-, Beratungs- und Überwachungsfunktion. Dabei ist er zudem durch den Verantwortlichen und Auftragsverarbeiter zu unterstützen. Er ist insofern Element der internen Selbstkontrolle. Damit verbunden ist keine Verlagerung der Verantwortung für die Einhaltung datenschutzrechtlicher Bestimmungen.

Zu Absatz 1:

Absatz 1 regelt die Aufgaben des Datenschutzbeauftragten im Anwendungsbereich der Verordnung (EU) 2016/679 nach § 1 Abs. 1 für Sachverhalte außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 (siehe § 2 Abs. 5) und für die in Ergänzung der Verordnung (EU) 2016/679 getroffenen Regelungen, wenn fachgesetzlich nichts anderes geregelt ist. Dabei stehen ihm die Aufgaben nach Artikel 39 Abs. 1 der Verordnung (EU) 2016/679 zu.

Von der Kontrolle ausgenommen ist aufgrund ihrer Unabhängigkeit die Personalvertretung.

Zu Absatz 2:

Nach Artikel 38 Abs. 1 der Verordnung (EU) 2016/679 und Artikel 33 Abs. 1 der Richtlinie (EU) 2016/680 ist der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Absatz 2 konkretisiert diese Vorgabe für den Fall des Verzeichnisses aller Verarbeitungstätigkeiten und der Datenschutz-Folgenabschätzung, da es sich um kom-

plexe Prozesse handelt, mit denen sich jeder Verantwortliche auseinandersetzen muss. Zwar führt der Verantwortliche das Verzeichnis aller Verarbeitungstätigkeiten. Um seiner Überwachungsfunktion nachkommen zu können, muss jedoch auch der Datenschutzbeauftragte Einsicht nehmen und gegebenenfalls Hinweise geben können. Im Falle der Datenschutz-Folgenabschätzung ist der Datenschutzberater schon bei der Beurteilung, ob eine solche durchzuführen ist, einzubinden. Die Beurteilung bemisst sich nach Artikel 35 Abs. 1 in Verbindung mit Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 beziehungsweise Artikel 27 Abs. 1 in Verbindung mit Artikel 19, 20 und 29 der Richtlinie (EU) 2016/680. Die Beteiligung des Datenschutzbeauftragten bei der Durchführung der Datenschutz-Folgenabschätzung richtet sich nach Artikel 35 Abs. 2 der Verordnung (EU) 2016/679 und Artikel 34 Buchst. c der Richtlinie (EU) 2016/680.

Zu Absatz 3:

Absatz 3 setzt Artikel 34 der Richtlinie (EU) 2016/680 um. Um die Aufgaben des Datenschutzbeauftragten für alle Verarbeitungszwecke einheitlich auszugestalten, entspricht die Bestimmung unter lediglich redaktioneller Anpassung Artikel 39 der Verordnung (EU) 2016/679.

Zu Absatz 4:

Absatz 4 entspricht Artikel 39 Abs. 2 der Verordnung (EU) 2016/679. Sie ist Ausdruck des risikobasierten Ansatzes der Verordnung (EU) 2016/679. Besonderes Gewicht hat der Datenschutzbeauftragte auf die mit der spezifischen Verarbeitung verbundene Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten der betroffenen Personen zu richten. Die Regelung hat keine Entsprechung in Artikel 34 der Richtlinie (EU) 2016/680, wird aber als allgemeiner Grundsatz festgeschrieben und als allgemeine Regelungen für die Bereiche außerhalb des Rechts der Europäischen Union festgelegt.

Zum Zweiten Abschnitt

Bestimmungen für die Verarbeitung zu Zwecken nach Artikel 2 der Verordnung (EU) 2016/679

Die Bestimmungen des Zweiten Abschnitts dienen ausschließlich der Umsetzung von Öffnungsklauseln und der Möglichkeiten zu Ausnahmeregelungen der Verordnung (EU) 2016/679 und damit ihrer Ergänzung hinsichtlich der Verarbeitung personenbezogener Daten sowie für solche Verarbeitungssituationen, die zwar nicht in den Anwendungsbereich der Verordnung fallen, auf welche aber aufgrund § 2 Abs. 5 die Verordnung sowie dieses Gesetz entsprechend anwendbar sind. Der Zweite Abschnitt ist immer in Ergänzung zu der Verordnung (EU) 2016/679 zu lesen, was durch die Klammerverweise deutlich wird. Sie deuten stets auf einzelne Bestimmungen hin, in deren Kontext oder aufgrund der dortigen Öffnungsklausel die landesrechtliche Regelung getroffen wurde.

Zum Ersten Unterabschnitt

Rechtsgrundlagen der Verarbeitung

Der Erste Unterabschnitt regelt die materiellen Voraussetzungen der Datenverarbeitung.

Zu § 16**Verarbeitung personenbezogener Daten (Artikel 6 und 9 der Verordnung (EU) 2016/679)**

§ 16 regelt die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten allgemein sowie für besondere Kategorien personenbezogener Daten in Ergänzung zu Artikel 6 und Artikel 9 der Verordnung (EU) 2016/679. Erfolgt die Datenverarbeitung nicht im Anwendungsbereich der Verordnung (EU) 2016/679, so ist diese nach § 2 Abs. 5 entsprechend anwendbar.

Zu Absatz 1:

Mit Absatz 1 wird eine Rechtsgrundlage für die Datenverarbeitung durch öffentliche Stellen auf der Grundlage von Artikel 6 Abs. 1 Buchst. e in Verbindung mit Artikel 6 Abs. 2 und 3 Satz 1 der Verordnung (EU) 2016/679 geschaffen. Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist nach der Bestimmung zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die ihr übertragen wurde. Neben den in Absatz 1 genannten Voraussetzungen ist jede Form der Datenverarbeitung auch unter den übrigen in Artikel 6 Abs. 1 der Verordnung (EU) 2016/679 genannten sonstigen Voraussetzungen sowie aufgrund spezialgesetzlicher Rechtsgrundlage auf Grundlage von Artikel 6 Abs. 1 Buchst. e der Verordnung (EU) 2016/679 zulässig.

Zu Absatz 2:

Absatz 2 regelt die Verarbeitung besonderer Kategorien personenbezogener Daten und dient der Umsetzung der in Artikel 9 Abs. 2 Buchst. g, j, b und h der Verordnung (EU) 2016/679 genannten Voraussetzungen für die Zulässigkeit der Verarbeitung dieser Datenkategorien. Die in Absatz 2 genannten Tatbestände gelten unbeschadet anderer Bestimmungen. Die Verarbeitung besonderer Kategorien personenbezogener Daten kann auch auf Grundlage von Artikel 9 Abs. 2 der Verordnung (EU) 2016/679 und anderen spezifischen Bestimmungen erfolgen. Durch Absatz 2 werden die Ausnahmetatbestände der bisherigen Regelung des § 4 Abs. 5 Nr. 5 bis 8 ThürDSG a. F. aufrechterhalten. Die bisherigen Nummern 1 bis 4 ergeben sich unmittelbar aus Artikel 9 Abs. 2 der Verordnung (EU) 2016/679.

Zu Satz 1:

Artikel 9 Abs. 2 Buchst. g, j, b und h der Verordnung (EU) 2016/679 setzen voraus, dass die Verarbeitung besonderer Kategorien personenbezogener Daten erforderlich ist und geeignete Garantien oder angemessene Maßnahmen für die betroffenen Personen vorgesehen sind. Durch die Formulierung "soweit und solange" wird sowohl eine inhaltliche als auch zeitliche Angemessenheitsprüfung statuiert.

Zu Nummer 1:

Nummer 1 regelt die Zulässigkeit der Datenverarbeitung zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und dient der Umsetzung von Artikel 9 Abs. 2 Buchst. g der Verordnung (EU) 2016/679.

Es handelt sich bei dem in der Verordnung (EU) 2016/679 verlangten erheblichen öffentlichen Interesses um einen auslegungsbedürftigen europarechtlich geprägten Begriff. Die Verordnung (EU) 2016/679 selbst definiert den Begriff nicht. In Erwägungsgrund 20 werden bestimmte öffentliche Interessen genannt, zu denen beispielhaft die öffentliche Sicherheit gehört. Erwägungsgründe 50 und 73 nennen das allgemeine öffentliche Interesse und beispielhaft dafür wirtschaftliche oder finanzi-

elle Interessen. Erwägungsgrund 112 schließlich erwähnt wichtige Gründe des öffentlichen Interesses und beispielhaft dafür den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten, beispielsweise im Falle der Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Verringerung und/oder Beseitigung des Dopings im Sport. Das erhebliche öffentliche Interesse im Sinne von Artikel 9 Abs. 2 Buchst. g der Verordnung (EU) 2016/679 stellt in diesem Gefüge ein gesteigertes Interesse der Öffentlichkeit dar. Nicht jede Angelegenheit stellt daher ein erhebliches öffentliches Interesse dar. Es muss sich um beträchtliche, ins Gewicht fallende Belange der Allgemeinheit handeln. Die in Nummer 1 genannten Gründe stellen jeweils ein erhebliches wichtiges öffentliches Interesse dar. Unter einem erheblichen öffentlichen Interesse im Sinne des Artikels 9 Abs. 2 Buchst. g der Verordnung (EU) 2016/679 werden damit auch die Abwehr von Gefahren für das Gemeinwohl und die öffentliche Sicherheit gefasst.

Zu Nummer 2:

Nummer 2 regelt die Datenverarbeitung zur Durchführung wissenschaftlicher oder historischer Forschung und dient der Umsetzung von Artikel 9 Abs. 2 Buchst. j der Verordnung (EU) 2016/679. Die Bestimmung entspricht zum Teil dem bisherigen Recht und wurde sprachlich an Artikel 5 und Artikel 89 der Verordnung (EU) 2016/679 angepasst.

Zu Nummer 3:

Nummer 3 regelt die Datenverarbeitung im Beschäftigungskontext, um den Rechten und Pflichten der öffentlichen Stellen auf dem Gebiet des Dienst- und Arbeitsrechts Rechnung zu tragen und dient der Umsetzung von Artikel 9 Abs. 2 Buchst. b der Verordnung (EU) 2016/679.

Zu Nummer 4:

Nummer 4 regelt die Datenverarbeitung zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung, der Behandlung oder für die Verwaltung von Gesundheitsdiensten und dient der Umsetzung von Artikel 9 Abs. 2 Buchst. h in Verbindung mit Abs. 3 der Verordnung (EU) 2016/679.

Zu Satz 2:

Satz 2 fasst für alle Ausnahmetatbestände die in Artikel 9 Abs. 2 der Verordnung (EU) 2016/679 genannten spezifischen Anforderungen an die Rechtsgrundlage zusammen.

Angemessene und spezifische Maßnahmen, beziehungsweise Garantien zur Wahrung der Grundrechte und Interessen der betroffenen Person können beispielsweise in geeigneten technischen und organisatorischen Maßnahmen im Sinne der Artikel 24, 25 und 32 der Verordnung (EU) 2016/679 bestehen. Die in Artikel 9 Abs. 2 Buchst. h und Absatz 3 der Verordnung (EU) 2016/679 geforderten besonderen Garantien werden unmittelbar durch § 16 Abs. 2 Nr. 4 umgesetzt und sind daher von Satz 2 ausgenommen. Weitere spezifische Maßnahmen zum Schutz der betroffenen Person ergeben sich aus den speziellen Rechtsgrundlagen für die Datenverarbeitung im Gesundheitsbereich.

Artikel 25 und 32 der Verordnung (EU) 2016/679 enthalten bereits Vorgaben zu den zu treffenden Maßnahmen. Die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ist sowohl bei Artikel 25 als auch Artikel 32 der Verordnung (EU) 2016/679 zu berücksichtigen. Bei der Verarbeitung besonders sensibler Daten sind die Maßnahmen also entsprechend durch besonders starke Schutzmechanismen auszufüllen.

Zu § 17**Zweckbindung und Zulässigkeit der Weiterverarbeitung (Artikel 6 und 23 der Verordnung (EU) 2016/679)**

§ 17 regelt die zulässigen Zwecke einer jeden Datenverarbeitung und die ausnahmsweise zulässige Weiterverarbeitung personenbezogener Daten zu anderen Zwecken als denjenigen, zu denen sie erhoben wurden. Dabei normiert Absatz 1, welche Zwecke stets vom originären Verarbeitungszweck umfasst sind und welche daher bereits keine Weiterverarbeitung darstellen. Absatz 2 bestimmt, welche Zwecke nach den Grundsätzen der Verordnung (EU) 2016/679 mit dem ursprünglichen Verwendungszweck vereinbar sind. Absatz 3 schließlich regelt diejenigen Zwecke, zu denen eine Weiterverarbeitung zu anderen Zwecken nie zulässig ist.

Da die Verordnung (EU) 2016/679 nur den Begriff der Verarbeitung verwendet und darunter nach Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 neben der Datenerhebung unter anderem auch die Datenübermittlung zählt, ist auch jede Übermittlung zukünftig eine Datenverarbeitung nach § 17 Abs. 1 oder 2. Von den Regelungen zur Zulässigkeit der Verarbeitung zu anderen Zwecken erfasst sind zukünftig auch die Fälle der Datenübermittlung an Stellen außerhalb des Verantwortlichen sowie die Weitergabe personenbezogener Daten innerhalb desselben. Sofern dies erforderlich ist, kann im Fachrecht weiterhin zwischen Datenerhebung und Datenübermittlung unterschieden werden, insbesondere kann die Übermittlung an bestimmte Stellen strengeren Voraussetzungen unterworfen werden.

Zu Absatz 1:

Absatz 1 nennt die Nebenzwecke, die stets vom originären Erhebungszweck umfasst sind und übernimmt die bisherige Bestimmung des § 20 Abs. 3 ThürDSG a. F. Es handelt sich um eine Fiktion, die es den öffentlichen Stellen ermöglicht, die ihnen obliegenden Aufsichts- und Kontrollaufgaben wahrzunehmen, ohne dass hierfür stets die Voraussetzungen für eine Datenerhebung nach der Verordnung (EU) 2016/679 vorliegen müssen. Mit Absatz 1 wird von Artikel 6 Abs. 1 Buchst. e, Abs. 2 und 3 der Verordnung (EU) 2016/679 Gebrauch gemacht. Demgemäß darf durch Rechtsvorschriften die Zweckbindung festgelegt werden, welcher die Verarbeitung personenbezogener Daten unterliegt. Die Regelung gilt daher nur für öffentliche Stellen, wenn die Datenverarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die ihr als Verantwortlichem übertragen wurde. Da es sich gerade nicht um eine Weiterverarbeitung zu anderen Zwecken handelt, kann eine Information nach Artikel 13 Abs. 3 und Artikel 14 Abs. 4 der Verordnung (EU) 2016/679 unterbleiben. Das Vorhalten von Back-up-Daten ist ausdrücklich von der Regelung erfasst.

Zu Absatz 2:

Absatz 2 regelt unter Berufung auf Artikel 6 Abs. 4 der Verordnung (EU) 2016/679 die Weiterverarbeitung zu anderen Zwecken als denen, zu denen die Daten erhoben wurden. Dies ist nur zulässig, wenn die betroffene Person eingewilligt hat oder die Weiterverarbeitung auf eine Rechtsgrundlage gestützt werden kann, die eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Abs. 1 der Verordnung (EU) 2016/679 genannten Ziele darstellt. Absatz 2 schafft hierfür landesrechtliche Rechtsgrundlagen und öffnet so die Möglichkeit eines Datenumgangs aus anderen als den ursprünglichen Erhebungszwecken. In den aufgeführten Fällen ist eine Einschränkung des Rechts

auf informationelle Selbstbestimmung aus überwiegenden Gründen des Gemeinwohls zulässig und geboten. Diese Regelungen sind entscheidend für den reibungslosen und rechtssicheren Datenfluss im Anwendungsbereich des Absatzes 2.

Zu Satz 1:

Satz 1 übernimmt die bisherigen Bestimmungen des § 20 Abs. 2 Nr. 3 bis 8 sowie des § 22 Abs. 1 Nr. 2 ThürDSG a. F. und passt diese in ihrer Formulierung, soweit notwendig, an die Anforderungen des Artikels 23 Abs. 1 der Verordnung (EU) 2016/679 an. Die Zulässigkeit der Weiterverarbeitung aufgrund einer Einwilligung folgt unmittelbar aus Artikel 6 Abs. 4 der Verordnung (EU) 2016/679, die Zulässigkeit aufgrund einer Rechtsvorschrift nach bisherigem Recht ist zu unspezifisch und erfüllt nicht die in Artikel 6 Abs. 4 der Verordnung (EU) 2016/679 genannten konkreten Anforderungen.

Zu Nummer 1:

Nummer 1 - die Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit - wird in Artikel 23 Abs. 1 Buchst. c und e der Verordnung (EU) 2016/679 als legitimes Ziel genannt.

Zu Nummer 2:

Nummer 2 lässt erforderliche Zweckänderungen zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne von § 11 Abs. 1 Nr. 8 StGB oder von Erziehungsmaßnahmen oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen zu. Die genannten Ziele werden in Artikel 23 Abs. 1 Buchst. d der Verordnung (EU) 2016/679 hinsichtlich der Verfolgung und Vollstreckung von Straftaten und in Buchstabe e hinsichtlich der Ordnungswidrigkeiten als legitimes Ziel genannt.

Zu Nummer 3:

Nummer 3 - der Schutz der Rechte und Freiheiten einer anderen Person - entspricht dem Wortlaut von Artikel 23 Abs. 1 Buchst. i der Verordnung (EU) 2016/679.

Zu Nummer 4:

Nach Nummer 4 ist die zweckändernde Weiterverarbeitung im Sinne einer Datenübermittlung an Dritte, die ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegen und wenn betroffene Personen kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben, zulässig. Nummer 4 entspricht der bisherigen Bestimmung des § 22 Abs. 1 Nr. 2 ThürDSG a. F., die bislang die Zulässigkeit der Datenübermittlung an nichtöffentliche Stellen festlegte. Nach neuer Rechtslage gilt die Bestimmung nun neben der Datenübermittlung an nichtöffentliche Stellen auch innerhalb des öffentlichen Bereichs. Der Begriff des Dritten wird in Artikel 4 Nr. 10 der Verordnung (EU) 2016/679 definiert.

Zu Nummer 5:

Nach Nummer 5 ist eine zweckändernde Weiterverarbeitung zulässig, wenn dies offensichtlich im Interesse der betroffenen Person liegt und wenn kein Grund zur Annahme besteht, dass die betroffene Person die Einwilligung hierzu verweigern würde. Es handelt sich dabei um einen legitimen Zweck im Sinne des Artikels 23 Abs. 1 Buchst. i der Verordnung (EU) 2016/679.

Zu Nummer 6:

Nummer 6 regelt Fälle, in denen offensichtliche Anhaltspunkte für die Unrichtigkeit der Angaben der betroffenen Person bestehen. Es handelt sich dabei um ein legitimes Ziel im Zusammenspiel aller Zielsetzungen von Artikel 23 Abs. 1 der Verordnung (EU) 2016/679.

Zu Nummer 7:

Nummer 7 regelt Fälle, in denen die Daten allgemein zugänglich sind oder die öffentliche Stelle sie veröffentlichen dürfte. Eine Auswertung allgemein zugänglicher Quellen kann insbesondere erforderlich sein zur Sicherstellung der öffentlichen Sicherheit, als auch zum Schutz der Rechte und Freiheiten einzelner Personen und finanziellen Interessen des Landes, etwa Steuerbetrug oder Sozialmissbrauch. Es handelt sich damit jedenfalls um ein legitimes Ziel der Weiterverarbeitung nach Artikel 23 Abs. 1 Buchst. c, e und i der Verordnung (EU) 2016/679.

Zu Nummer 8:

Nummer 8 soll nach Artikel 23 Abs. 1 Buchst. e der Verordnung (EU) 2016/679 sicherstellen, dass, sofern öffentliche Stellen personenbezogene Daten im Zusammenhang mit steuerrelevanten Sachverhalten erhalten, diese weiterverarbeiten können.

Zu Satz 2:

Satz 2 stellt klar, dass auch eine Weiterverarbeitung zu Archiv-, Forschungs- und Statistikzwecken nach Artikel 5 Abs. 1 Buchst. b der Verordnung (EU) 2016/679 stets kompatibel ist. Artikel 5 Abs. 1 Buchst. b der Verordnung (EU) 2016/679 geht im Rahmen einer Fiktion davon aus, dass die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke immer zweckkompatibel ist.

Zu Satz 3:

Über die Bestimmung der Sätze 1 und 2 in Absatz 2 hinaus ist die Weiterverarbeitung nach Artikel 6 Abs. 4 der Verordnung (EU) 2016/679 dann zulässig, wenn sie mit dem ursprünglichen Zweck vereinbar ist. Dieser Fall der Zweckkompatibilität bedarf nach Erwägungsgrund 50 keiner eigenen Rechtsgrundlage. Die Bewertung der Vereinbarkeit obliegt dem Verantwortlichen, wobei unter anderem die in Artikel 6 Abs. 4 der Verordnung (EU) 2016/679 und die in Erwägungsgrund 50 genannten Grundsätze zu berücksichtigen sind.

Zu Satz 4:

Für den Fall, dass eine zweckändernde Weiterverarbeitung zur Verfolgung der in Artikel 23 Abs. 1 der Verordnung (EU) 2016/679 genannten Ziele zugelassen wurde, normiert Satz 4, dass eine Informationspflicht gegenüber der betroffenen Person nicht besteht, solange und soweit der Zweck der Verarbeitung durch eine solche Information gefährdet würde. Nach Artikel 23 Abs. 1 der Verordnung (EU) 2016/679 können die Rechte und Pflichten nach den Artikeln 12 bis 22 und 34 der Verordnung (EU) 2016/679 beschränkt werden, soweit dies erforderlich ist, um die in Artikel 23 Abs. 1 Buchst. a bis j der Verordnung (EU) 2016/679 genannten Ziele sicherzustellen. Sobald eine Gefährdungssituation durch zeitliche oder sachliche Erledigung nicht mehr besteht, hat eine Information an die betroffene Person zu erfolgen.

Zu Absatz 3:

Absatz 3 bestimmt, dass bei personenbezogenen Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbei-

tungsanlage verarbeitet werden, eine Weiterverarbeitung zu anderen Zwecken stets unzulässig ist. Die Bestimmung entspricht der Regelung des bisherigen § 20 Abs. 4 ThürDSG a. F. und wird gerechtfertigt durch Artikel 6 Abs. 2 und 3 der Verordnung (EU) 2016/679. Demgemäß darf durch Rechtsvorschriften die Zweckbindung festgelegt werden, denen personenbezogene Daten unterliegen.

Für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke ist eine Weiterverarbeitung stets zulässig, da Artikel 5 Abs. 1 Buchst. b der Verordnung (EU) 2016/679 nicht abbedungen werden kann. Gleiches gilt für die Weiterverarbeitung zu den in Absatz 1 genannten Zwecken.

Zu § 18

Übermittlung (Artikel 6 Abs. 2 der Verordnung (EU) 2016/679)

§ 18 regelt die Rechte und Pflichten im Zusammenhang mit der Datenübermittlung. Zwar handelt es sich um eine Datenverarbeitung, die nach Artikel 6 und hinsichtlich der Rechte und Pflichten insbesondere in Kapitel III der Verordnung (EU) 2016/679 geregelt ist, die Verordnung (EU) 2016/679 enthält aber keine ausdrückliche Regelung zur Verantwortlichkeit bei Datenübermittlungen.

Im Unterschied zur bisherigen Rechtslage gilt § 18 sowohl bei der Datenübermittlung im öffentlichen Bereich als auch zwischen öffentlichen und nichtöffentlichen Stellen.

Zu Absatz 1:

Absatz 1 legt den für die Übermittlung Verantwortlichen fest und bestimmt dessen Pflichten. Die Bestimmung entspricht der bisherigen Regelung in § 21 Abs. 2 und § 22 Abs. 2 ThürDSG a. F., da die Verordnung grundsätzlich nicht zwischen öffentlichen und nichtöffentlichen Stellen unterscheidet. Die Regelungsbefugnis ergibt sich aus Artikel 4 Nummer 7 der Verordnung (EU) 2016/679, der es den Mitgliedstaaten der Europäischen Union gestattet, den Verantwortlichen zu bestimmen oder Modalitäten seiner Benennung festzulegen.

Zu Absatz 2:

Absatz 2 regelt, dass die Übermittlung von personenbezogenen Daten zulässig ist, wenn sie untrennbar verbunden oder nur mit unververtretbarem Aufwand trennbar sind mit den zu übermittelnden Daten nach Absatz 1. Es handelt sich bei Absatz 2 um eine spezifische Bestimmung nach Artikel 6 Abs. 2 der Verordnung (EU) 2016/679, ohne die bereits die Verarbeitung der tatsächlich erforderlichen Daten nicht möglich wäre. Indem die Nutzung der zusätzlich übermittelnden Daten unzulässig ist, wird auch eine Verarbeitung nach Treu und Glauben gewährleistet, die den Rechten aller betroffenen Personen und Dritter gerecht wird.

Zu Absatz 3:

Bei einer Datenübermittlung mittels eines automatisierten Verfahrens trägt die abrufende Stelle, also der Empfänger, die Verantwortung. Absatz 3 entspricht der bisherigen Regelung des § 21 Abs. 5 ThürDSG a. F. Hintergrund ist, dass im Rahmen eines automatisierten Abrufs die speichernde Stelle von dem Abruf regelmäßig keine Kenntnis erlangt. Die Regelungsbefugnis folgt aus Artikel 4 Nr. 7 der Verordnung (EU) 2016/679. Die Mitgliedstaaten der Europäischen Union können den Verantwortlichen einer Datenverarbeitung bestimmen.

Zu § 19**Auftragsverarbeitung (Artikel 28 der Verordnung (EU) 2016/679)**

§ 19 ergänzt die Bestimmungen zur Auftragsverarbeitung in Artikel 28 der Verordnung (EU) 2016/679.

Zu Absatz 1:

Absatz 1 stellt klar, dass auch dann, wenn der Auftragsverarbeiter nicht in den Anwendungsbereich fällt, die Regeln zur Auftragsverarbeitung nach der Verordnung (EU) 2016/679 sowie die ergänzenden Regelungen Anwendung finden. Absatz 1 ergänzt die Bestimmung des § 2 Abs. 5, indem er zusätzlich regelt, wer für die Einhaltung der Bestimmungen der Verordnung (EU) 2016/679 verantwortlich ist.

Zu Absatz 2:

Durch Absatz 2 wird die bisherige Bestimmung des § 8 Abs. 2 Satz 5 ThürDSG a. F. übernommen und so die Möglichkeit geschaffen, dass die zuständige Fachaufsichtsbehörde zum Vertragsabschluss bevollmächtigt werden kann.

**Zum Zweiten Unterabschnitt
Rechte der betroffenen Person**

Kapitel III der Verordnung (EU) 2016/679 enthält Bestimmungen zu den Rechten der betroffenen Person. Dabei handelt es sich um

- die Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person nach Artikel 13 der Verordnung (EU) 2016/679,
- die Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden nach Artikel 14 der Verordnung (EU) 2016/679,
- das Auskunftsrecht der betroffenen Person nach Artikel 15 der Verordnung (EU) 2016/679,
- das Recht auf Berichtigung nach Artikel 16 der Verordnung (EU) 2016/679,
- das Recht auf Löschung („Recht auf Vergessenwerden“) nach Artikel 17 der Verordnung (EU) 2016/679,
- das Recht auf Einschränkung der Verarbeitung nach Artikel 18 der Verordnung (EU) 2016/679,
- die Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung nach Artikel 19 der Verordnung (EU) 2016/679,
- das Recht auf Datenübertragbarkeit nach Artikel 20 der Verordnung (EU) 2016/679,
- das Widerspruchsrecht nach Artikel 21 der Verordnung (EU) 2016/679,
- das grundsätzliche Verbot automatisierter Entscheidungen im Einzelfall einschließlich Profiling nach Artikel 22 der Verordnung (EU) 2016/679 und
- die Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person nach Artikel 34 der Verordnung (EU) 2016/679.

Dabei sind die Rechte nach den Artikeln 16, 19, 20, 21 und 22 der Verordnung (EU) 2016/679 für öffentliche Stellen bereits abschließend geregelt. Im Übrigen werden durch die §§ 20 ff. Regelungen zu den Betroffenenrechten getroffen, welche die Verordnung um bisher geltende Bestimmungen des ThürDSG a. F. ergänzen. Kapitel III der Verordnung (EU) 2016/679 enthält darüber hinaus mit Artikel 12 eine einleitende Bestim-

mung, welche die Modalitäten festlegt, welche für die betroffene Person bei Geltendmachung ihrer Rechte sowie für den Verantwortlichen gelten.

Zu § 20

Informationspflichten (Artikel 13, 14 und 23 der Verordnung (EU) 2016/679)

§ 20 regelt in Ergänzung zu den Artikeln 13 und 14 der Verordnung (EU) 2016/679 die Beschränkung der Informationspflichten gegenüber der betroffenen Person bei der Datenverarbeitung sowie die Informationspflicht gegenüber nichtöffentlichen Stellen.

Zu Absatz 1:

Durch die Regelung werden die Ausnahmen von der Auskunftspflicht nach bisherigem Recht aufrechterhalten.

Die Informationspflichten gegenüber der betroffenen Person werden nach dem System der Verordnung (EU) 2016/679 in den Artikeln 13 und 14 abhängig davon geregelt, ob die Daten bei der betroffenen Person oder bei einer anderen Stelle erhoben wurden. Damit verbunden werden lediglich unterschiedliche Informationspflichten. Daher kann das Primat der Direkterhebung nach § 19 Abs. 2 ThürDSG a. F. nicht aufrechterhalten werden, da die Verordnung (EU) 2016/679 keine Abstufung dahingehend vornimmt.

Während Artikel 13 die Informationspflicht bei Datenerhebung bei der betroffenen Person regelt, normiert Artikel 14 die Informationspflicht, wenn die Datenerhebung nicht bei der betroffenen Person erfolgt. Artikel 14 enthält bereits Ausnahmetatbestände. Artikel 23 der Verordnung (EU) 2016/679 lässt darüber hinaus weitere und gemeinsame Ausnahmen von den Informationspflichten zu.

Artikel 23 Abs. 1 der Verordnung (EU) 2016/679 setzt dabei voraus, dass die Beschränkung nur dann zulässig ist, sofern sie den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und eine notwendige und verhältnismäßige Maßnahme darstellt. Der Verantwortliche hat zu prüfen, in welchem Umfang und für welchen Zeitraum eine entsprechende Ausnahme besteht. Liegt ein Ausnahmetatbestand nicht mehr vor, ist die entsprechende Information zu erteilen ("soweit und solange").

Zu Nummer 1:

Ziel von Nummer 1 ist es, die vielseitigen staatlichen Interessen gegenüber einer bedingungslosen Offenlegung an betroffene Personen zu schützen.

Die Ausnahmeregelung ist gerechtfertigt durch Artikel 23 Abs. 1 Buchst. c und e der Verordnung (EU) 2016/679. Die Begriffe "öffentliche Sicherheit" und "Wohle des Bundes oder eines Landes" sind europarechtskonform im Lichte der Verordnung (EU) 2016/679 auszulegen.

Zu Nummer 2:

Nummer 2 entspricht inhaltlich der bisherigen Bestimmung in § 13 Abs. 5 Nr. 3 ThürDSG a. F. und enthält zwei Fallgruppen. Zunächst wird die Ausnahme aufgrund der Geheimhaltungsbedürftigkeit wegen Rechtsvorschriften bestimmt. Es handelt sich um eine zulässige Beschränkung nach Artikel 23 Abs. 1 Buchst. e der Verordnung (EU) 2016/679.

Zum anderen wird die Ausnahme zum Schutz der Rechte und Freiheiten anderer Personen geregelt. Die Regelungsbefugnis folgt aus Artikel 23 Abs. 1 Buchst. i der Verordnung (EU) 2016/679.

Zu Nummer 3:

Nummer 3 regelt im Unterschied zum bisherigen Recht eine zusätzliche Ausnahme von den Informationspflichten. Damit wird ein Gleichlauf

mit den Ausnahmen von der Informationspflicht nach der Richtlinie (EU) 2016/680 und deren Umsetzung im Landesrecht erreicht.

Zu Absatz 2:

Absatz 2 normiert, dass für Daten, die ausschließlich zu Zwecken der Datensicherung oder der Datenschutzkontrolle verarbeitet werden, keine Pflicht zur Information besteht. Der Verantwortliche kann aber im Rahmen des Ermessens prüfen, ob dennoch eine Information erfolgen soll. Die Bestimmung entspricht der Ausnahme von den Auskunftspflichten nach bisherigem Recht und soll durch die Verortung bei der Beschränkung von den Informationspflichten den Gleichlauf der Ausnahmetatbestände sicherstellen. Die Regelungsbefugnis folgt aus Artikel 23 Abs. 1 Buchst. h der Verordnung (EU) 2016/679.

Die unter Absatz 2 genannten Daten beeinträchtigen das Persönlichkeitsrecht der betroffenen Personen typischerweise nicht. Es handelt sich um Daten, die im Rahmen von technischen und organisatorischen Maßnahmen und im Rahmen der Sicherstellung des Datenschutzes verarbeitet werden. Die Beschränkung unter Absatz 2 gilt nur, wenn die Daten ausschließlich zu den genannten Zwecken verarbeitet werden.

Zu Absatz 3:

Absatz 3 regelt den Umfang der Informationspflicht gegenüber den nicht-öffentlichen Stellen und entspricht der bisherigen Bestimmung in § 19 Abs. 4 ThürDSG a. F. Die Verordnung (EU) 2016/679 enthält keine Regelungen zur Information gegenüber Dritten, bei denen die Daten erhoben werden. Die nichtöffentlichen Stellen sollen zumindest die Informationen erhalten, die ihnen die Entscheidung ermöglicht, die verlangten Angaben zu machen oder sie zu verweigern.

Zu § 21

Auskunftsrecht (Artikel 15 und 23 der Verordnung (EU) 2016/679)

§ 21 ergänzt die Regelung des Artikels 15 der Verordnung (EU) 2016/679 in Anwendung der Öffnungsklausel des Artikels 23 der Verordnung (EU) 2016/679 um Ausnahmen vom Auskunftsanspruch der betroffenen Personen. Da die Verordnung (EU) 2016/679 auch für Papierakten gilt, sofern sie nach bestimmten Kriterien geordnet sind (siehe dazu Erwägungsgrund 15), sind besondere Regelungen zum Umgang mit dem Auskunftsanspruch nicht mehr erforderlich.

Zu Absatz 1:

Absatz 1 regelt die Ausnahmen vom Auskunftsanspruch nach Artikel 15 der Verordnung (EU) 2016/679. Die Bestimmung übernimmt zum Teil die bisherige Bestimmung des § 13 Abs. 5 ThürDSG a. F., soweit die dort normierten Ausnahmetatbestände unter Artikel 23 der Verordnung (EU) 2016/679 subsumiert werden können.

In allen aufgeführten Fallgruppen ist nach Artikel 23 der Verordnung (EU) 2016/679 eine Verhältnismäßigkeitsprüfung vorzunehmen. Eine Beschränkung des Auskunftsanspruchs kann deshalb nur bestehen, soweit und solange die unter den Nummern 1 bis 3 aufgeführten Interessen den berechtigten Interessen der betroffenen Person vorgehen. Der Verantwortliche hat zu prüfen, in welchem Umfang und für welchen Zeitraum eine entsprechende Ausnahme besteht. Liegt ein Ausnahmetatbestand nicht mehr vor, ist die entsprechende Auskunft zu erteilen. Die Bestimmung entspricht § 20 Abs. 1 und regelt die gleichen Ausnahmetatbestände für den Zeitpunkt der Auskunftserteilung.

Zu Absatz 2:

Absatz 2 regelt die Ausnahme vom Auskunftsanspruch, wenn die Daten ausschließlich zu Zwecken der Datensicherung und Datenschutzkontrolle gespeichert sind. Absatz 2 übernimmt die bisherige Regelung des § 13 Abs. 1 Satz 2 ThürDSG a. F. Damit wird zudem der Gleichlauf der Ausnahmetatbestände mit den Informationsrechten verwirklicht (vergleiche § 20 Abs. 2).

Zu Absatz 3:

Absatz 3 bestimmt Fallgruppen, in denen die Auskunftserteilung im Zusammenhang mit der Übermittlung personenbezogener Daten nur mit Zustimmung des Empfängers (Staatsanwaltschaft, Polizeibehörden, Verfassungsschutzbehörde, Bundesnachrichtendienst, Militärischer Abschirmdienst und andere Behörden des Bundesministeriums der Verteidigung) zulässig ist. Dies entspricht der bisherigen Regelung in § 13 Abs. 4 ThürDSG a. F. Es wird damit dem Geheimhaltungsbedürfnis der genannten Stellen und dem Umstand Rechnung getragen, dass regelmäßig nur die genannten Stellen aufgrund ihrer Sachnähe eine sachlich informierte Entscheidung über den Auskunftsanspruch treffen können. Eine Regelungsbefugnis ergibt sich aus dem Umstand, dass Sicherheitsbehörden nicht dem Anwendungsbereich der Verordnung (EU) 2016/679 (Artikel 2 Abs. 2 der Verordnung (EU) 2016/679) unterfallen und damit vom Anwendungsbereich des zweiten Unterabschnitts ausgenommen werden können.

Satz 2 ergänzt die Regelung des Satzes 1 um die Datenübermittlung von den genannten Behörden. Auch im Falle der Datenübermittlung von Behörden mit besonderen Geheimhaltungsinteressen besteht die Gefahr, dass deren Interesse an einer Geheimhaltung unterlaufen wird, wenn an den Empfänger ein Auskunftsbegehren gerichtet wird.

Zu Absatz 4:

Satz 1 bestimmt, dass die Verweigerung, der betroffenen Person Auskunft zu gewähren, keiner Begründung bedarf, soweit und solange dadurch der Zweck der Auskunftsverweigerung gefährdet würde und entspricht der bisherigen Bestimmung in § 13 Abs. 6 ThürDSG a. F. Sind durch die Begründung Rückschlüsse auf die geheimhaltungsbedürftigen Umstände möglich, die zur ursprünglichen Ablehnung des Auskunftsbegehrens geführt haben, soll eine Begründung unterbleiben, um den Zweck von Absatz 2 und 3 nicht zu gefährden. Die Regelungsbefugnis ergibt sich als Annex aus Artikel 23 der Verordnung (EU) 2016/679. Werden Beschränkungen der Betroffenenrechte vorgenommen, müssen auch flankierende Maßnahmen zur effektiven Wirkung der Beschränkungen zulässig sein.

Zu Satz 2:

Zur Wahrnehmung ihrer berechtigten Interessen kann sich die betroffene Person an den Landesbeauftragten für den Datenschutz wenden. Es handelt sich bei Satz 2 um eine Präzisierung der Regelung in Artikel 57 Abs. 1 Buchst. e der Verordnung (EU) 2016/679.

Zu Absatz 5:

Absatz 5 bestimmt, dass dem Landesbeauftragten für den Datenschutz auf Verlangen der betroffenen Person hin Auskunft zu erteilen ist. Die Beschränkung der Auskunft an den Landesbeauftragten dient dem Schutz der öffentlichen Sicherheit (Artikel 23 Abs. 1 Buchst. c der Verordnung (EU) 2016/679) und der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten (Artikel 23 Abs. 1 Buchst. d der Verordnung (EU) 2016/679).

Zu § 22**Recht auf Einschränkung der Verarbeitung (Artikel 18 der Verordnung (EU) 2016/679)**

§ 22 ergänzt die Regelung in Artikel 18 der Verordnung (EU) 2016/679 zum Recht auf Einschränkung der Verarbeitung und nutzt dabei die gegebene Möglichkeit, die "wichtigen öffentlichen Interessen", bei deren Vorliegen eine Verarbeitung trotz Einschränkung zulässig ist, zu konkretisieren. Es handelt sich bei den Nummern 1 bis 4 um Regelbeispiele, nicht um eine abschließende Aufzählung.

Durch § 22 sollen die nach bereits bisherigem Recht geltenden Ausnahmen von der Verarbeitungssperre aufrechterhalten bleiben, sofern sie sich nicht bereits unmittelbar aus Artikel 18 Abs. 2 der Verordnung (EU) 2016/679 ergeben. Die sich aus dem bisherigen Recht ergebenden Ausnahmen zu Zwecken der Behebung einer bestehenden Beweisnot und aus sonstigen im überwiegenden Interesse eines Dritten liegenden Gründen wurden nicht übernommen, da sie sich unmittelbar aus Artikel 18 Abs. 2 der Verordnung (EU) 2016/679 ergeben. Die Ausnahme aus sonstigen im überwiegenden Interesse der Datenverarbeitenden Stelle liegenden Gründen wurde nicht übernommen, da sie sich nicht durch die Verordnung (EU) 2016/679 rechtfertigen lässt.

Zu Nummer 1:

Nach Nummer 1 ist eine Verarbeitung personenbezogener Daten trotz Einschränkung zu wissenschaftlichen und historischen Forschungszwecken zulässig. Dabei sind jedoch wiederum die Bedingungen des § 16 Abs. 2 Nr. 2 zu berücksichtigen, sofern besondere Kategorien personenbezogener Daten verarbeitet werden.

Zu Nummer 2:

Nummer 2 nimmt entsprechend der Systematik der Verordnung (EU) 2016/679 Archivzwecke als wichtiges öffentliches Interesse auf.

Zu Nummer 3:

Nummer 3 regelt Fallgruppen, in denen in der Regel Daten nur verwaltungsintern verarbeitet werden und dies die betroffenen Personen nicht nachteilig berührt. Weiterhin kann die Nutzung personenbezogener Daten zur Aufklärung möglicher Datenschutzverstöße beitragen, die möglicherweise auch Grund für die Einschränkung waren.

Zu Nummer 4:

Nummer 4 bestimmt ebenfalls eine Fallgruppe, in welcher in der Regel Daten nur verwaltungsintern verarbeitet werden und dies die betroffenen Personen nicht nachteilig berührt. Weiterhin dient die Rechnungsprüfung letztlich auch den Interessen der betroffenen Personen.

Zu § 23**Löschung personenbezogener Daten (Artikel 17 der Verordnung (EU) 2016/679)**

§ 23 ergänzt die Regelung in Artikel 17 Abs. 1 Buchst. e der Verordnung (EU) 2016/679 zur Löschung personenbezogener Daten.

Personenbezogene Daten sind vor einer Löschung dem zuständigen Archiv anzubieten, die Entscheidung des Archivs ist abzuwarten. Das Thüringer Archivgesetz regelt das Verfahren zum Anbieten und Aussondern des Archivguts. Die Regelung übernimmt die bisherige Bestimmung in § 16 Abs. 3 ThürDSG a. F.

Die Regelung des § 23 basiert auf Artikel 17 Abs. 3 Buchst. d der Verordnung (EU) 2016/679. Personenbezogene Daten sind dann nicht un-

verzüglich zu löschen, wenn dies die Verwirklichung von im öffentlichen Interesse liegenden Archivzwecken unmöglich macht oder ernsthaft erschwert. Zur Bewertung müssen die Daten zunächst dem Archiv angeboten werden.

Zu § 24

Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person (Artikel 34 der Verordnung (EU) 2016/679)

§ 24 regelt in Anwendung von Artikel 23 der Verordnung (EU) 2016/679 weitere Ausnahmen von der Benachrichtigungspflicht gegenüber der betroffenen Person und ergänzt §§ 20 Abs. 1 und 21 Abs. 1. Wenn bereits eine Information oder Auskunft über die Datenverarbeitung an die betroffene Person aus bestimmten Gründen nicht erfolgt, so muss dasselbe auch für die Benachrichtigungspflicht gelten.

Satz 1 benennt die Fallkonstellationen, in denen eine Benachrichtigung von der Verletzung des Schutzes personenbezogener Daten der betroffenen Personen unterbleiben kann. Eine Ausnahme von der Benachrichtigungspflicht muss sich aber immer daran messen lassen, ob sie in dem Umfang tatsächlich inhaltlich und zu dem Zeitpunkt erforderlich und angemessen ist. Die unbedingte, also zeitlich unbegrenzte und inhaltlich allumfassende Ausnahme von der Benachrichtigungspflicht kann daher nur die letzte aller möglichen Maßnahmen sein, die Information nach Artikel 34 der Verordnung (EU) 2016/679 einzuschränken ("soweit und solange").

Zu Nummer 1 bis 3:

Die Nummern 1 bis 3 entsprechen den Regelungen in § 20 Abs. 1 und § 21 Abs. 1.

Zu Nummer 4:

Nummer 4 enthält unabhängig von den Tatbeständen der §§ 20 Abs. 1 und 21 Abs. 1 eine weitere Ausnahme von der Benachrichtigungspflicht für den Fall, dass durch die Benachrichtigung die Sicherheit von IT-Systemen gefährdet wird. Erfasst sind Sachverhalte, in denen eine Datenverarbeitung fehlerhaft und damit der Schutz personenbezogener Daten nicht erfolgreich war. Durch die Offenbarung punktueller oder großflächiger Schutzlücken gegenüber den betroffenen Personen könnte möglicherweise das IT-System im Einzelfall von außen (Bsp. Hackerangriff) angreifbar werden.

Zum Dritten Unterabschnitt Besondere Verarbeitungssituationen

Zu § 25

Verarbeitung personenbezogener Daten zu Zwecken der freien Meinungsäußerung und der Informationsfreiheit

Aufgrund der überragenden Bedeutung von Information und freier Kommunikation für die Demokratie ist es zielführend, nicht nur die Arbeit "traditioneller" Medien in der Form journalistisch-redaktionell operierender Unternehmen mit den Regelungen zum Datenschutz in Einklang zu bringen, sondern entsprechend Artikel 85 Abs. 1 der Verordnung (EU) 2016/679 auch andere, vergleichbare Datenverarbeitungsvorgänge wegen ihrer Bedeutung für die Informations- und Kommunikationsfreiheit in ebenso vergleichbarer Weise zu privilegieren.

Zu § 26**Öffentliche Stellen, die am Wettbewerb teilnehmen**

§ 26 schreibt vor, welche Bestimmungen auf die öffentlichen Stellen, die am Wettbewerb teilnehmen, anwendbar sind. Da es sich noch immer um öffentliche Stellen des Landes handelt, verbleibt die Aufsicht bei dem Thüringer Landesbeauftragten für den Datenschutz.

Der Grundsatz der Wettbewerbsgleichheit verlangt aber zugleich, dass öffentliche Stellen, die am Wettbewerb teilnehmen, den privaten Wettbewerbsteilnehmern gleichgestellt sind. Nach der Struktur des nationalen Datenschutzrechts wird daher in Satz 2 Teil 2 des Bundesdatenschutzgesetzes für anwendbar erklärt.

Zu § 27**Datenschutz im Beschäftigungskontext (Artikel 88 der Verordnung (EU) 2016/679)**

§ 27 regelt den Datenschutz im Beschäftigtenverhältnis. Artikel 88 der Verordnung (EU) 2016/679 enthält Bestimmungen zum Beschäftigten-datenschutz in nationalen Regelungen und eröffnet dem Gesetzgeber auf diesem Gebiet Handlungsmöglichkeiten. Die Mitgliedstaaten der Europäischen Union können nach Artikel 88 Abs. 1 der Verordnung (EU) 2016/679 spezifische Bestimmungen zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz, des Schutzes des Eigentums der Arbeitgeber oder der Kunden sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses vorsehen.

§ 27 übernimmt weitestgehend die bisherige Regelung des § 33 ThürDSG a. F. Die Regelungen der Absätze 2 bis 4 sind notwendig, da sie den Schutz der Daten von Bewerbern regeln, bei denen es zu keiner Einstellung gekommen ist und daher das Thüringer Beamtenengesetz (ThürBG) keine Anwendung findet.

Zu Absatz 1:

Zunächst stellt Absatz 1 Arbeitnehmer und Auszubildende öffentlicher Stellen datenschutzrechtlich den Beamten gleich und erklärt für diese die Bestimmungen des Thüringer Beamtengesetzes über das Führen von Personalakten für anwendbar, es sei denn, besondere Bestimmungen finden Anwendung. Das Thüringer Beamtengesetz regelt den Umgang mit personenbezogenen Daten in personalrechtlichen Angelegenheiten für Landesbeamte abschließend. Es handelt sich dabei um eine spezialgesetzliche Ausprägung des in Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 2 Grundgesetz verankerten Schutzes des allgemeinen Persönlichkeitsrechts im Hinblick auf den Umgang mit personenbezogenen Daten im Personalrecht, also einen bereichsspezifischen Datenschutz. Bereits das Bundesverwaltungsgericht hat betont, dass es sich bei den beamtenrechtlichen Bestimmungen zum Datenschutz um abschließende Sonderregelungen handelt, die ein umfassendes Regelungssystem über den Umgang mit Personaldaten bilden (BVerwG, Urteil vom 27.02.2003 - 2 C 10.02). Gleichwohl wurden bestimmte Sachverhalte (Auftragsdatenverarbeitung) im Thüringer Beamtengesetz bisher nicht geregelt.

Aufgrund der Bestimmung des § 2 Abs. 4 wird die Gefahr einer Regelungslücke geschlossen. Allgemeine Bestimmungen des Datenschutzgesetzes und der Verordnung (EU) 2016/679 finden stets Anwendung, soweit spezialgesetzlich keine Regelung getroffen wurde.

Eine datenschutzrechtliche Regelung, dass dies auch für Arbeitnehmer und Auszubildende gilt, ist erforderlich, da das Thüringer Beamtengesetz in diesen Formen des Beschäftigungsverhältnisses keine unmittelbare Anwendung findet.

Die Regelungsbefugnis folgt aus Artikel 88 Abs. 1 der Verordnung (EU) 2016/679, der eine genauere Definition des Beschäftigtenbegriffs zulässt.

Zu Absatz 2:

Absatz 2 stellt nach Erwägungsgrund 155 eine besondere Bestimmung über die formellen Bedingungen dar, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage einer Einwilligung der Beschäftigten verarbeitet werden dürfen. Das grundsätzliche Schriftformerfordernis kann im Einzelfall auch durch andere Form der Einwilligung ersetzt werden. Dies kommt etwa im Falle von elektronischen Bewerbungsverfahren in Betracht.

Darüber hinaus ist nach den Erwägungsgründen 42 und 43 zu beachten, dass Einwilligungen nur freiwillig erteilt werden können. Dies ist insbesondere im Beschäftigungskontext aufgrund des möglichen Ungleichgewichts zwischen den Parteien sorgfältig zu berücksichtigen. Bei dieser Beurteilung können insbesondere die im Beschäftigungsverhältnis grundsätzlich bestehende Abhängigkeit der oder des Arbeitnehmers vom Arbeitgeber und die Umstände des Einzelfalls zu berücksichtigen sein.

Zu Absatz 3:

Absatz 3 bestimmt, dass das Verarbeiten personenbezogener Daten, die bei medizinischen oder psychologischen Untersuchungen zum Zwecke der Eingehung des Beschäftigungsverhältnisses erhoben wurden, nur mit schriftlicher Einwilligung des Bewerbers zulässig ist. Satz 1 stellt dabei nicht ausdrücklich nur auf sensible Daten im Sinne des Artikels 9 der Verordnung (EU) 2016/679 ab. Gleichwohl werden typischerweise bei medizinischen und psychologischen Tests besonders sensible Kategorien personenbezogener Daten abgefragt.

Die Regelungsbefugnis ergibt sich aus Artikel 6 in Verbindung mit Artikel 88 Abs. 1 und 2 der Verordnung (EU) 2016/679. Demgegenüber bestimmt Satz 2, welche Daten aus den Untersuchungen nach Satz 1 dem Arbeitgeber gegenüber stets übermittelt werden dürfen.

Zu Absatz 4:

Absatz 4 stellt klar, dass personenbezogene Daten in der Regel unverzüglich zu löschen sind, sobald feststeht, dass das Beschäftigungsverhältnis nicht zustande kommt und die Frist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen abgelaufen ist (beispielsweise § 15 Abs. 4 Allgemeines Gleichbehandlungsgesetz). In dem Fall entfällt der Zweck, der mit der Datenerhebung verbunden war. Damit wird im Rahmen des Beschäftigungskontexts klargestellt, dass die Löschung unverzüglich und ohne ausdrückliches Verlangen der betroffenen Person zu erfolgen hat.

Zu Absatz 5:

Absatz 5 regelt die Zweckbindung von Daten, die zur Durchführung technischer und organisatorischer Maßnahmen nach Artikel 32 der Verordnung (EU) 2016/679 gespeichert worden sind. Es handelt sich um Datenspeicherungen im Zusammenhang mit den durch den Verantwortlichen zu treffenden technischen und organisatorischen Maßnahmen zum Schutz

der Verarbeitungsmaßnahmen. Diese Daten dürfen nicht zu Zwecken der Verhaltens- und Leistungskontrolle genutzt werden. Es handelt sich um eine spezialgesetzliche Ausgestaltung der Zweckbindung auf Grundlage von Artikel 88 Abs. 1 der Verordnung (EU) 2016/679.

Zu § 28

Verarbeitung personenbezogener Daten durch Forschungseinrichtungen (Artikel 6, 9 und 89 der Verordnung (EU) 2016/679)

§ 28 regelt die Verarbeitung personenbezogener Daten durch öffentliche Forschungseinrichtungen und übernimmt weitestgehend die bisherigen Regelungen.

Erfasst sind davon sowohl wissenschaftliche als auch historische Forschungsvorhaben. Von der Regelung unberührt bleibt Artikel 5 Abs. 1 Buchst. b der Verordnung (EU) 2016/679. Die Weiterverarbeitung personenbezogener Daten zu wissenschaftlichen und historischen Zwecken ist unabhängig davon, ob es sich bei der verarbeitenden Stelle um eine Forschungseinrichtung handelt, zulässiger Verarbeitungszweck.

Zu Absatz 1:

Eine Verarbeitung zu anderen Zwecken wird für die zur wissenschaftlichen oder historischen Forschung erhobenen Daten ausgeschlossen. Dies soll sicherstellen, dass personenbezogene Daten im Rahmen der Forschungsverwendung verbleiben. Eine Zweckbindung auf konkrete Forschungsvorhaben ist von dem Verbot jedoch nicht erfasst. Eine Datenverarbeitung zu anderen wissenschaftlichen oder historischen Forschungsvorhaben ist damit nicht ausgeschlossen.

Absatz 1 ist gerechtfertigt durch Artikel 6 Abs. 1 Buchst. e in Verbindung mit Abs. 3 der Verordnung (EU) 2016/679.

Zu Absatz 2:

Durch Absatz 2 wird die Übermittlung personenbezogener Daten an Stellen, die nicht dem Anwendungsbereich dieses Gesetzes oder der Verordnung (EU) 2016/679 unterfallen, an bestimmte formelle Voraussetzungen geknüpft. Der Datenempfänger muss eine besondere Verpflichtungserklärung abgeben, mit der er erklärt, ebenfalls die Regelung der Zweckbindung nach Absatz 1 zu beachten, die Daten zu anonymisieren und die Bestimmungen über die Veröffentlichung zu beachten.

Zu Absatz 3:

Nach Absatz 3 hat eine Anonymisierung personenbezogener Daten zu erfolgen, sobald dies nach dem Forschungszweck möglich ist. Die Regelungsbefugnis folgt aus Artikel 89 Abs. 1 der Verordnung (EU) 2016/679, wonach die Verarbeitung personenbezogener Daten zu Forschungszwecken geeigneten Garantien zum Schutz der betroffenen Person unterliegt. Die Definition des Begriffs "anonymisieren" entspricht der Definition in § 3 Abs. 9 ThürDSG a. F.

Auch schon vor der möglichen Anonymisierung sind personenbezogene Daten getrennt zu speichern, um sie einer Einzelperson nicht zuzuordnen zu können. Gemeint ist die Trennung von Sachdaten und Identifikationsmerkmalen.

Einzelangaben dürfen zur Erreichung des Forschungszwecks nur zusammengeführt werden, wenn dies erforderlich ist.

Zu Absatz 4:

Nach Absatz 4 ist eine Veröffentlichung personenbezogener Daten zulässig, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung der Forschungsergebnisse über Personen der Zeitgeschichte unerlässlich ist. Die vollständige und korrekte Darstellung muss unverzichtbar sein.

Da es sich bei der Veröffentlichung um eine Form der Verarbeitung handelt (vgl. Artikel 4 Nr. 2 der Verordnung (EU) 2016/679), stellt Absatz 4 eine Einschränkung der Verarbeitung dar, die gerechtfertigt wird durch Artikel 6 Abs. 1 Buchst. e und Artikel 6 Abs. 3 der Verordnung (EU) 2016/679.

Zu Absatz 5:

Absatz 5 schränkt die Rechte der betroffenen Person ein, soweit und solange die Verwirklichung des Forschungsinteresses durch Umsetzung der Betroffenenrechte unmöglich gemacht oder nachträglich beeinträchtigt wird.

Zu § 29

Zweckbindung von personenbezogenen Daten, die einem Berufsgeheimnis unterliegen (Artikel 6 und 9 der Verordnung (EU) 2016/679)

§ 29 regelt die Verarbeitung von personenbezogenen Daten, die einem Berufsgeheimnis unterliegen. Adressat der Norm ist der Verantwortliche, welchem die Daten von der zur Verschwiegenheit verpflichteten Stelle übermittelt worden sind, der jedoch selbst keinem solchen Geheimnis unterliegt. Die personenbezogenen Daten behalten nach § 29 dabei ihren besonderen Schutz.

Die Regelungsbefugnis folgt aus Artikel 6 Abs. 1 Buchst. e in Verbindung mit Artikel 6 Abs. 3 der Verordnung (EU) 2016/679.

Zu Absatz 1:

Nach Absatz 1 unterliegen diese personenbezogenen Daten dem Zweck, für welchen sie dem Verantwortlichen von dem Berufspflichtträger übermittelt worden sind.

Gegenüber der bisherigen Bestimmung in § 24 Abs. 1 ThürDSG a. F. wurden lediglich redaktionelle Änderungen vorgenommen. Außerdem wurde das Kriterium des Amtsgeheimnisses, welchem die personenbezogenen Daten neben dem Berufsgeheimnis auch unterliegen konnten, gestrichen, da die Verordnung (EU) 2016/679 nicht zwischen Berufs- und besonderem Amtsgeheimnis unterscheidet.

Zu Absatz 2:

Eine Weiterverarbeitung zu anderen Zwecken auf der Grundlage von § 17 Abs. 2 ist für diese Daten ausgeschlossen. Davon unberührt bleibt die Weiterverarbeitung aufgrund einer Rechtsvorschrift, die den Anforderungen aus Artikel 6 Abs. 4 in Verbindung mit Artikel 23 der Verordnung (EU) 2016/679 genügt. Dies entspricht der bisherigen Regelung. Die Regelungsbefugnis ergibt sich aus Artikel 6 Abs. 2 und 3 der Verordnung (EU) 2016/679, in welchen geregelt wird, welcher Zweckbindung bestimmte Daten unterliegen.

Zu § 30

Videoüberwachung

§ 30 regelt die Zulässigkeit und die Voraussetzungen der Videobeobachtung oder -aufzeichnung durch öffentliche Stellen.

Zu Absatz 1:

Absatz 1 regelt die Zulässigkeit der Videobeobachtung (Datenerhebung) und -aufzeichnung (Speicherung).

Die Verordnung (EU) 2016/679 regelt den Fall der Videoüberwachung nicht speziell, vielmehr handelt es sich um eine allgemeine Art der Datenverarbeitung durch öffentliche Stellen nach Artikel 6 Abs. 1 Buchst. e und Abs. 2 der Verordnung (EU) 2016/679.

Die Beobachtung und Aufzeichnung ist nur zulässig, soweit sie zum Schutz von Personen bzw. des Eigentums oder des Besitzes an Sachen - diese Rechtsgüter stehen in einem so engen Zusammenhang, dass sie einen einheitlichen Zweck darstellen - erforderlich ist. Die Erforderlichkeit ergibt sich aus dem Schutz der Rechtsgüter. Die in Absatz 1 Nr. 1 und 2 genannten Rechtsgüter können nur soweit durch Videoüberwachung geschützt werden, als damit gleichzeitig auch eine Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt verfolgt wird. Eine Aufgabe im öffentlichen Interesse stellt insbesondere auch die Aufrechterhaltung der Funktionsfähigkeit öffentlicher Stellen und ihrer Gebäude dar, also die Möglichkeit des ungestörten Benutzerverkehrs und der ungestörten Nutzung.

Zudem enthält Absatz 1 eine Definition der Videoüberwachung. Optisch-elektronische Einrichtungen sind alle Geräte, die Bilder übertragen und aufzeichnen. Der Begriff der Einrichtung erfordert dabei eine zumindest vorübergehende ortsgebundene Installation. Eine Speicherung ist ausdrücklich nicht Voraussetzung für die Anwendbarkeit der Bestimmung. Ebenso ist nicht Voraussetzung, dass die erhobenen Daten einer bestimmten Person zugeordnet werden können.

Durch die ausdrückliche Normierung der Schutzgüter Leben, Gesundheit oder Freiheit in Satz 3 wird diesen im Rahmen der Interessenabwägung ein besonderes Gewicht gegeben. Ein ergebnisoffener Abwägungsprozess hat gleichwohl auch weiterhin stattzufinden.

Ausdrückliches Ziel der Bestimmung ist die Erhöhung der Sicherheit in sämtlichen öffentlichen Stellen, (siehe dazu § 2). Insbesondere fallen darunter Einrichtungen des öffentlichen Personennahverkehrs - sofern diese dem Anwendungsbereich dieses Gesetzes unterfallen - da dort aufgrund der hohen Frequentierung und Gefahrenanfälligkeit Sicherheitsbelange von besonderer Bedeutung sind.

Zu Absatz 2:

Absatz 2 enthält eine spezifische Bestimmung zur Ausprägung des Transparenzgebots nach Artikel 5 Abs. 1 Buchst. a der Verordnung (EU) 2016/679. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Allerdings müssen im Falle der Videoüberwachung nicht sämtliche Informationen unmittelbar zur Verfügung gestellt werden, sondern aus Praktikabilitätsgründen nur die in Artikel 13 Abs. 1 Buchst. a bis c der Verordnung (EU) 2016/679 genannten. Es handelt sich dabei um Informationen zu dem Verantwortlichen sowie seinem Vertreter, die Kontaktdaten des Datenschutzbeauftragten sowie die Zwecke, für welche die Daten verarbeitet werden sollen und die Rechtsgrundlage für die Verarbeitung.

In dem Hinweis über die Videoüberwachung ist darüber hinaus ausdrücklich darauf hinzuweisen, wo die betroffenen Personen die weiteren Informationen nach Artikel 13 der Verordnung (EU) 2016/679 erhalten können. Mit dem Hinweis auf den Verantwortlichen ist die öffentliche Stelle gemeint, die selbst erhebt oder im Auftrag erheben lässt.

Zu Absatz 3:

Durch den Einsatz von Videoüberwachung erhobene Daten dürfen nur verarbeitet werden, wenn dies zum Erreichen des verfolgten Zwecks erforderlich ist und unter Berücksichtigung des Schutzes von Leben, Gesundheit oder Freiheit von Personen, die sich in der überwachenden Stelle aufhalten, keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. Durch Absatz 3 sollen für die Videoüberwachung und die Verwendung der erhobenen Daten die

gleichen Maßstäbe gelten. Als erhoben gelten Daten bei der Videoaufzeichnung, aber auch bei der zufälligen Informationswahrnehmung und unaufgeforderten Informationszuleitung. Die Regelung gilt unabhängig vom Personenbezug der erhobenen Daten. Absatz 3 entspricht der bisherigen Regelung in § 25a Abs. 3 ThürDSG a. F. Die Regelungsbefugnis zur Zweckbindung folgt aus Artikel 6 Abs. 3 der Verordnung (EU) 2016/679.

Zu Absatz 4:

Absatz 4 enthält eine von § 17 und Artikel 6 Abs. 4 der Verordnung (EU) 2016/679 abweichende Regelung zur Zweckbindung. Eine über den Erhebungszweck hinausgehende Weiterverarbeitung zu anderen Zwecken ist nur zulässig, wenn dies zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder zur Verfolgung von Straftaten erforderlich ist. Hierbei geht es insbesondere um die Übermittlung an die für die Verfolgung von Straftaten und Ordnungswidrigkeiten zuständigen Behörden. Ob eine Ordnungswidrigkeit erhebliche Bedeutung hat, ist eine Frage der Einzelfallabwägung und hängt ab von den Auswirkungen eines Verstoßes, dem Gewicht der beeinträchtigten Rechtsgüter, die Art und Höhe der Sanktion et cetera.

Die Regelung entspricht der bisherigen Bestimmung in § 25a Abs. 3 Satz 2 ThürDSG a. F.

Zu Absatz 5:

Videoaufzeichnungen und aus der Videoüberwachung erhobene personenbezogene Daten sind nach Artikel 17 Abs. 1 der Verordnung (EU) 2016/679 unverzüglich zu löschen, wenn sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind. Dies gilt nur dann nicht, wenn sie zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder zur Verfolgung von Straftaten oder zur Geltendmachung von Rechtsansprüchen benötigt werden. Es handelt sich insofern um eine Ausnahme von Artikel 17 Abs. 1 der Verordnung (EU) 2016/679, welche durch Artikel 23 Abs. 1 Buchst. d, e und i der Verordnung (EU) 2016/679 gerechtfertigt ist.

Zum Dritten Abschnitt

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

Zum Ersten Unterabschnitt

Anwendungsbereich und Grundsätze

Zu § 31

Anwendungsbereich (Artikel 1 Abs. 1, Artikel 2 Abs. 1 der Richtlinie (EU) 2016/680)

Der Dritte Abschnitt dient im Wesentlichen der Umsetzung der Richtlinie (EU) 2016/680. § 31 regelt dabei den Anwendungsbereich. Er gilt nur für Verarbeitungen durch öffentliche Stellen und, vgl. Artikel 3 Nr. 7 Buchst. b der Richtlinie (EU) 2016/680 und § 2 Abs. 2, als öffentliche Stellen geltende Beliehene, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit zuständig sind und auch nur, soweit sie zu diesen Zwecken Daten verarbeiten. Dies sind insbesondere die Polizeibehörden, die Staatsanwaltschaften und die Steuerfahndung, soweit sie die Daten zu den genannten Zwecken verarbeiten. Dies schließt Gefahrenabwehrzwecke ein. Weiterhin erfasst sind auch kommunale Vollstreckungsstellen (nach § 36 ThürVwZVG die Kassen der Gemeinden, Landkreise, kreisfreien Städ-

te, Verwaltungsgemeinschaften oder Zweckverbände), jedenfalls sofern sie Forderungen aus Ordnungswidrigkeiten vollstrecken.

Für die Eröffnung des Anwendungsbereichs des Dritten Abschnitts und damit auch der Richtlinie (EU) 2016/680 genügt also eine Verarbeitung zu den oben genannten Zwecken allein nicht; daneben muss auch eine grundsätzliche Befugnis- und Aufgabenzuweisung (Zuständigkeit) für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit vorliegen.

Die Ermittlung, Verfolgung und Ahndung von Ordnungswidrigkeiten sowie die Vollstreckung von in Ordnungswidrigkeitenverfahren festgesetzten Geldbußen und angeordneten Nebenfolgen sind vom Anwendungsbereich umfasst; dies wird durch Erwägungsgrund 13 der Richtlinie (EU) 2016/680 unterstützt. Hierdurch wird insbesondere erreicht, dass die polizeiliche Datenverarbeitung einheitlichen Regeln folgt, unabhängig davon, ob eine Straftat oder eine Ordnungswidrigkeit in Rede steht. Der Dritte Abschnitt des vorliegenden Gesetzes gilt damit auch für Behörden, die nicht Polizeibehörden sind, soweit sie aber Ordnungswidrigkeiten verfolgen, ahnden und in einem Ordnungswidrigkeitenverfahren festgesetzte Geldbußen und angeordnete Nebenfolgen vollstrecken. Dabei muss die Datenverarbeitung auch sonstigen Regeln folgen, welche die Richtlinie (EU) 2016/680 umsetzen. Daraus folgt, dass die Datenverarbeitung bei Verwaltungsbehörden, wie zum Beispiel Waffen-, Hygiene- oder Passbehörden, deren Aufgabenzuweisung nicht mit den in § 31 genannten Zwecken übereinstimmt, grundsätzlich solange und soweit nicht in den Anwendungsbereich der Richtlinie und damit des Dritten Abschnitts fällt, wie die von ihnen geführten Verfahren nicht in ein konkretes Ordnungswidrigkeitenverfahren übergehen.

Auftragsverarbeiter, deren Tätigkeit sich grundsätzlich dadurch auszeichnet, dass sie Daten zur Erfüllung einer Auftragsverarbeitungsvereinbarung und nicht aufgrund eigener Aufgabenzuschreibung verarbeiten, sind durch die Regelungen des Dritten Abschnitts nur adressiert, sofern sie konkret angesprochen sind. Die von ihnen durchgeführten Verarbeitungen richten sich im Übrigen nach den Regelungen der Verordnung (EU) 2016/679 bzw. den diese ausformenden Ersten und Zweiten Abschnitt. Das schließt nicht aus, dass durch den Dritten Abschnitt angesprochene Verantwortliche auch als Auftragsverarbeiter tätig sein können.

Zu § 32

Begriffsbestimmungen (Artikel 3 der Richtlinie (EU) 2016/680)

Die Begriffsbestimmungen in den Nummern 1 bis 16 sind zum Zwecke der Umsetzung der Richtlinie (EU) 2016/680 aufgenommen worden. Sie schließen an die Begriffsbestimmungen in Artikel 3 der Richtlinie (EU) 2016/680 und hinsichtlich des in Nummer 14 aufgeführten Begriffs "besondere Kategorien personenbezogener Daten" an Artikel 10 der Richtlinie (EU) 2016/680 an.

Zu § 33

Grundsätze bei der Verarbeitung personenbezogener Daten (Artikel 8, Artikel 4 Abs. 2 und 3, Artikel 9 Abs. 2 und 3 der Richtlinie (EU) 2016/680)

Zu Absatz 1:

Die Verarbeitung ist nur zulässig, wenn sie für die Aufgabenerfüllung erforderlich ist und keine spezielleren Regelungen in anderen Geset-

zen vorgehen. Die Bestimmung setzt Artikel 4 Abs. 1 der Richtlinie (EU) 2016/680 um.

Zu Absatz 2:

Satz 1 setzt Artikel 4 Abs. 2 der Richtlinie (EU) 2016/680 um. Somit wird klargestellt, dass Verantwortliche Daten so lange und so weit zu anderen Zwecken, als zu denen sie ursprünglich erhoben wurden, verarbeiten dürfen, so lange es sich bei diesen anderen Zwecken um einen in § 31 genannten Zweck handelt und diese Verarbeitung erforderlich und verhältnismäßig ist. Grundsätzlich eröffnet Artikel 4 Abs. 2 der Richtlinie (EU) 2016/680 stets die Möglichkeit, die Daten für einen der in § 31 genannten Zwecke zu verarbeiten und innerhalb der Palette der genannten Zwecke auch Zweckänderungen vorzunehmen, wobei der EU-Gesetzgeber offen lässt, ob in diesen Fällen überhaupt eine Zweckänderung vorliegt. Zusätzliche Anforderungen an die Zweckänderung innerhalb der in § 31 genannten Zwecke müssen in den Fachgesetzen umgesetzt werden, dies gilt zum Beispiel für die aus der verfassungsgerichtlichen Rechtsprechung zum Polizeirecht resultierenden gesteigerten Anforderungen an schwerwiegende Grundrechtseingriffe.

Satz 2 betrifft die Weiterverarbeitung von zu Zwecken des § 31 erhobenen Daten zu anderen als in § 31 genannten Zwecken. Eine solche ist zulässig, wenn dies in einer Rechtsvorschrift vorgesehen ist.

Zu Absatz 3:

Absatz 3 greift Artikel 4 Abs. 3 der Richtlinie (EU) 2016/680 auf, wonach Verantwortliche Daten auch zu Archivzwecken, wissenschaftlichen, statistischen und historischen Zwecken verarbeiten dürfen, solange diese Verarbeitung unter die in § 31 genannten Zwecke gefasst werden kann.

Zu § 34

Unterscheidung verschiedener Kategorien betroffener Personen sowie zwischen Tatsachen und Bewertungen (Artikel 6, Artikel 7 Abs. 1 der Richtlinie (EU) 2016/680)

Zu Absatz 1:

Absatz 1 dient der Umsetzung von Artikel 6 der Richtlinie (EU) 2016/680. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, etwa der Unterscheidung entsprechender Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Maßnahmen der Datensicherheit, werden dem jeweiligen Fachgesetz überlassen.

Zu Absatz 2:

Absatz 2 dient der Umsetzung von Artikel 7 Abs. 1 der Richtlinie (EU) 2016/680. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, etwa der Unterscheidung entsprechender Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besonderer Maßnahmen der Datensicherheit, werden dem Fachrecht überlassen.

Zu § 35

Berichtigung und Löschung personenbezogener Daten sowie die Einschränkung der Verarbeitung (Artikel 4 Abs. 1, Artikel 7 Abs. 3, Artikel 5 der Richtlinie (EU) 2016/680)

§ 35 dient der Umsetzung von Artikel 4 Abs. 1 Buchst. d der Richtlinie (EU) 2016/680. Systematisch werden in § 35 Pflichten des Verantwortlichen zur Berichtigung und Löschung personenbezogener Daten sowie zur Einschränkung ihrer Verarbeitung thematisiert, die unabhängig davon bestehen, ob eine betroffene Person darum nachsucht. Die spiegel-

bildlich bestehenden Rechte der betroffenen Person auf Berichtigung, Löschung personenbezogener Daten sowie auf Einschränkung der Verarbeitung durch den Verantwortlichen finden sich in § 43.

Zu Absatz 1:

In Absatz 1 wird die Pflicht des Verantwortlichen zur Berichtigung unrichtiger Daten auch ohne Antrag der betroffenen Person statuiert.

Zu Absatz 2:

Absatz 2 regelt die in Artikel 16 Abs. 2 der Richtlinie (EU) 2016/680 normierte Pflicht des Verantwortlichen zur Löschung.

Zu Absatz 3:

Absatz 3 benennt abschließend die Konstellationen, bei denen an die Stelle einer Löschung eine Verarbeitungseinschränkung treten kann. Die durch Nummer 3 eröffnete Möglichkeit, von der Löschung wegen unverhältnismäßigen Aufwands abzusehen, wird aus der derzeitigen Rechtslage übernommen (vergleiche § 16 Abs. 4 Nr. 2 ThürDSG a. F.). Diese Bestimmung ist dabei als restriktiv auszulegende Ausnahmeregelung anzusehen. Im Grundsatz sollte die bei Verantwortlichen zum Einsatz kommende IT-Infrastruktur darauf ausgelegt sein, eine Lösungsverpflichtung auch technisch nachvollziehen zu können.

Zu Absatz 4:

Absatz 4 dient der Umsetzung von Artikel 7 Abs. 3 der Richtlinie (EU) 2016/680.

Zu Absatz 5:

Absatz 5 setzt Artikel 5 Satz 2 der Richtlinie (EU) 2016/680 um.

Zu § 36

Verfahren bei Übermittlungen (Artikel 7 Abs. 2, Artikel 9 Abs. 3 und 4 der Richtlinie (EU) 2016/680)

Zu Absatz 1:

Die Bestimmung dient der Umsetzung von Artikel 7 Abs. 2 der Richtlinie (EU) 2016/680. Im Hinblick auf die Vervollständigung unvollständiger Daten als möglichem Sinn und Zweck einer Datenübermittlung wurde die in der Richtlinie (EU) 2016/680 enthaltene Vermeidung der Übermittlung "unvollständiger" Daten nicht übernommen. Ferner ist bei der Anwendung und Auslegung der Anforderungen des § 36 zu beachten, dass sich die Frage nach der "Aktualität" von Daten und der damit verbundenen Vorgabe, keine "nicht mehr aktuellen" Daten zu übermitteln beziehungsweise bereitzustellen, stets nur im konkreten Ermittlungszusammenhang und unter Beachtung des konkreten Verarbeitungszwecks beantworten lässt. In bestimmten Ermittlungszusammenhängen kann auch die Übermittlung nicht (mehr) aktueller Daten, wie alte Meldeadressen, alte (Geburts-)Namen et cetera, bedeutsam und für die Aufgabenerfüllung erforderlich sein.

Zu Absatz 2:

Absatz 2 wiederum setzt Artikel 9 Abs. 3 der Richtlinie (EU) 2016/680 um. Beispiele für die im Fachrecht vorgesehene Mitgabe besonderer Bedingungen können Zweckbindungsregelungen bei der Weiterverarbeitung durch den Empfänger oder das Verbot der Weiterübermittlung ohne Genehmigung oder Konsultationserfordernisse vor der Beauskunftung betroffener Personen durch den Empfänger sein.

Zu Absatz 3:

Absatz 3 setzt Artikel 9 Abs. 4 der Richtlinie (EU) 2016/680 um.

Zu § 37

Verarbeitung besonderer Kategorien personenbezogener Daten (Artikel 10 der Richtlinie (EU) 2016/680)

§ 37 dient der Umsetzung von Artikel 10 der Richtlinie (EU) 2016/680.

Zu Absatz 1:

Absatz 1 legt fest, dass die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist und schafft damit eine eigene Rechtsgrundlage für diese Verarbeitungen. Das kann auch die Verarbeitung in den in Artikel 10 Buchst. b und c der Richtlinie (EU) 2016/680 genannten Zusammenhängen, das heißt zur Wahrung lebenswichtiger Interessen der betroffenen Person oder eines Dritten oder wenn Daten verarbeitet werden sollen, die die betroffene Person offensichtlich öffentlich gemacht hat, umfassen.

Zu Absatz 2:

In Absatz 2 wird in Satz 1 klargestellt, dass bei der Verarbeitung geeignete Garantien für die Rechtsgüter der betroffenen Personen beachtet werden müssen.

In Satz 2 werden beispielhaft mögliche geeignete Garantien aufgeführt. Die konkrete Ausgestaltung der Maßnahmen kann also von Einzelfall zu Einzelfall variieren.

Zu § 38

Automatisierte Einzelentscheidung (Artikel 11 der Richtlinie (EU) 2016/680)

§ 38 setzt Artikel 11 der Richtlinie (EU) 2016/680 um und regelt das Verbot auf automatisierter Verarbeitung basierender Einzelentscheidungen. Um eine in Absatz 1 genannte, nur unter bestimmten Umständen zulässige, "Entscheidung, die eine nachteilige Rechtsfolge für die betroffene Person hat", zu sein, muss es sich bei einer solchen Entscheidung um einen Rechtsakt mit Außenwirkung gegenüber der betroffenen Person - regelmäßig einen Verwaltungsakt - handeln. Interne Zwischenfestlegungen oder -auswertungen, die Ausfluss automatisierter Prozesse sind, fallen nicht hierunter.

Zu § 39

Einwilligung

In § 39 finden sich die Voraussetzungen für eine wirksame Einwilligung. Hierbei wurden Elemente aus Artikel 7 der Verordnung (EU) 2016/679 mit dort nicht enthaltenen Elementen des § 4 ThürDSG a. F. kombiniert.

Zum Zweiten Unterabschnitt Rechte der betroffenen Person

Zu § 40

Allgemeiner Informationsanspruch (Artikel 13 Abs. 1 der Richtlinie (EU) 2016/680)

§ 40 dient der Umsetzung von Artikel 13 Abs. 1 der Richtlinie (EU) 2016/680. Es geht hier um aktive Informationspflichten des Verantwortlichen gegenüber betroffenen Personen unabhängig von der Geltendmachung von Betroffenenrechten. Dieser Informationspflicht sollen Verant-

wortliche in allgemeiner Form nachkommen können. Durch die explizit in Erwägungsgrund 42 der Richtlinie (EU) 2016/680 aufgenommene Möglichkeit der Information über die Internetseite des Verantwortlichen wird der Sinn und Zweck der Regelung im Zusammenhang klargestellt: Betroffene Personen sollen sich unabhängig von der Datenverarbeitung im konkreten Fall in leicht zugänglicher Form einen Überblick über die Zwecke der beim Verantwortlichen durchgeführten Verarbeitungen verschaffen können und eine Übersicht über die ihnen zu Gebote stehenden Betroffenenrechte bekommen.

Zu § 41

Benachrichtigung betroffener Personen (Artikel 13 Abs. 2 und 3 der Richtlinie (EU) 2016/680)

§ 41 betrifft Fälle, in denen in fachgesetzlichen Regelungen eine aktive Benachrichtigung betroffener Personen vorgesehen ist. Eine Festlegung dieser in Artikel 13 Abs. 2 der Richtlinie (EU) 2016/680 so bezeichneten "besonderen Fälle" ist nicht verallgemeinernd auf Ebene des Thüringer Datenschutzgesetzes möglich und muss somit im Fachrecht geleistet werden. Leitend für die Entscheidung, ob eine Benachrichtigung unabhängig von der Geltendmachung eines Betroffenenrechts angezeigt ist, dürfte zum Beispiel sein, ob die Verarbeitung mit oder ohne Wissen der betroffenen Person, gegebenenfalls in Verbindung mit einer erhöhten Eingriffstiefe, erfolgt. In letztgenannten Fällen ist eine aktive, gegebenenfalls nachträgliche Benachrichtigung die einzige Möglichkeit für die betroffene Person, von der Verarbeitung Kenntnis zu erlangen und gegebenenfalls deren Rechtmäßigkeit mithilfe der Geltendmachung von Betroffenenrechten zu prüfen.

Zu Absatz 1:

Absatz 1 stellt klar, welche Informationen betroffenen Personen von dem Verantwortlichen in diesen Fällen aktiv übermittelt werden müssen und dient dabei der Umsetzung von Artikel 13 Abs. 2 der Richtlinie (EU) 2016/680.

Zu Absatz 2:

Absatz 2 ermöglicht es in Umsetzung von Artikel 13 Abs. 3 der Richtlinie (EU) 2016/680, zu den dort genannten Zwecken von der Bereitstellung der in Absatz 1 genannten Informationen abzusehen, sie einzuschränken oder sie aufzuschieben. Den Ausnahmen ist der Gedanke gemein, dass die Auskunftserteilung nicht zur Gefährdung der ordnungsgemäßen Erfüllung der Aufgaben des Verantwortlichen führen soll.

Die Nutzung der Möglichkeit, von der Bereitstellung der in Absatz 1 genannten Informationen abzusehen, sie einzuschränken oder aufzuschieben, muss Verhältnismäßigkeitsgrundsätzen genügen, mithin in ein angemessenes Verhältnis zur Bedeutung der Betroffeneninformation für die spätere Geltendmachung von Betroffenenrechten gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen, ob die Bereitstellung etwa nur teil- oder zeitweise eingeschränkt werden kann ("so weit und solange").

Zu Absatz 3:

Absatz 3 statuiert ein Zustimmungserfordernis der dort genannten Stellen, wenn sich die Benachrichtigung auf die Übermittlung an diese Stellen (nach Absatz 1 Satz 1 Nummer 4) bezieht. Insofern besteht ein der Situation der aktiven Geltendmachung von Betroffenenrechten vergleichbarer Sachverhalt, weshalb die Übernahme geboten ist. Die Bestimmung ist ausschließlich im Zusammenhang mit fachgesetzlichen Regelungen anzuwenden. Diese sehen zum Beispiel in § 36 Abs. 4 ThürPAG eine Abstimmung mit der Staatsanwaltschaft zwingend vor.

Zu § 42**Auskunftsrecht (Artikel 14 bis 17 der Richtlinie (EU) 2016/680)**

§ 42 regelt das Auskunftsrecht als zentrales Betroffenenrecht und normiert gleichzeitig dessen Einschränkungen. Die Bestimmung dient mit hin der Umsetzung der Artikel 14 (Bestehen des Auskunftsrechts) und 15 (Ausnahmen) der Richtlinie (EU) 2016/680. Das Auskunftsrecht setzt - im Gegensatz zu in § 41 angesprochenen aktiven Benachrichtigungspflichten - einen entsprechenden Antrag der betroffenen Person voraus, in dem sowohl die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, als auch der Grund des Auskunftsverlangens angegeben werden soll.

Zu Absatz 1:

Absatz 1 legt den Umfang des der betroffenen Person zustehenden Auskunftsrechts fest. Der in den Nummern 1 und 4 genannte Begriff "Kategorie" ermöglicht dem Verantwortlichen eine angemessene Generalisierung der Angaben zu den verarbeiteten personenbezogenen Daten sowie zu den Übermittlungsempfängern. Die Angaben nach Nummer 1 zu den verarbeiteten personenbezogenen Daten können im Sinne einer zusammenfassenden Übersicht in verständlicher Form gemacht werden. Die Angaben müssen also nicht in einer Form gemacht werden, welche Aufschluss über die Art und Weise der Speicherung oder Sichtbarkeit der Daten beim Verantwortlichen (im Sinne einer Kopie) zulässt. Ebenso bedeutet die Pflicht zur Angabe der verfügbaren Informationen zur Datenquelle nicht, dass die Identität natürlicher Personen oder gar vertrauliche Informationen preisgegeben werden müssen. Der Verantwortliche muss sich bei der Angabe zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, letztlich von dem gesetzgeberischen Ziel leiten lassen, bei der betroffenen Person ein Bewusstsein über Umfang und Art der verarbeiteten Daten zu erzeugen und es ihr ermöglichen, aufgrund dieser Informationen zu ermessen, ob die Verarbeitung rechtmäßig ist und - wenn Zweifel hieran bestehen - gegebenenfalls die Geltendmachung weiterer Betroffenenrechte auf diese Informationen stützen zu können. Im letzten Satz wird die bisherige Regelung des § 13 Abs. 4 ThürDSG a. F. übernommen.

Zu Absatz 2:

Absatz 2 überführt den Rechtsgedanken des bisherigen § 13 Abs. 1 Satz 2 ThürDSG a. F. in das Thüringer Datenschutzgesetz.

Zu Absatz 3:

Absatz 3 überführt die Bestimmung des bisherigen § 13 Abs. 3 Satz 2 ThürDSG a. F. in dieses Gesetz.

Zu Absatz 4:

Absatz 4 normiert, zu welchen Zwecken das Auskunftsrecht durch den Verantwortlichen vollständig oder teilweise eingeschränkt werden darf. Die Bestimmung geht zum Schutz der betroffenen Person über das durch die Richtlinie (EU) 2016/680 Gebotene hinaus, indem tatbestandlich jeweils eine Gefährdung - gegenüber einer in der Richtlinie angesprochenen Beeinträchtigung - der genannten Rechtsgüter oder Zwecke vorausgesetzt wird. Den Ausnahmen ist der Gedanke gemein, dass die Auskunftserteilung nicht zur Gefährdung der ordnungsgemäßen Erfüllung der Aufgaben des Verantwortlichen führen soll. Die Nutzung der Möglichkeit, von der Auskunftserteilung vollständig oder teilweise abzu sehen, muss Verhältnismäßigkeitsgrundsätzen genügen und ihr muss eine nachvollziehbare Interessenabwägung vorausgehen. Die durch das teilweise oder vollständige Absehen von der Auskunftserteilung ge-

geschützten Rechtsgüter müssen mithin in ein angemessenes Verhältnis zur Bedeutung der Auskunftserteilung für die spätere Geltendmachung weiterer Betroffenenrechte gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen, ob die Auskunft etwa nur teilweise eingeschränkt oder zu einem späteren Zeitpunkt erteilt werden kann.

Zu Absatz 5:

Absatz 5 Sätze 1 und 2 dienen der Umsetzung von Artikel 15 Abs. 3 Sätze 1 und 2 der Richtlinie (EU) 2016/680. Hierdurch wird dem Verantwortlichen - auch gemeinsam mit der sich aus Absatz 4 ergebenden Variante, die Frage nach dem "Ob" der Verarbeitung nicht zu beantworten - die Möglichkeit gegeben, das Auskunftsverlangen unbeantwortet zu lassen. Satz 3 nimmt in Bezug auf das Absehen von einer Begründung der Auskunftsverweigerung zusätzlich einen aus § 13 Abs. 6 Satz 1 ThürDSG a. F. entnommenen Gedanken auf.

Zu Absatz 6:

Absatz 6 regelt die Möglichkeiten, die der betroffenen Person im Fall des Absehens von einer Begründung für die vollständige oder teilweise Einschränkung des Auskunftsrechts oder im Fall der überhaupt ausbleibenden Beantwortung des Auskunftsverlangens bleiben. Nach Satz 1 kann die betroffene Person ihr Auskunftsrecht nach Auskunftsverweigerung durch den Verantwortlichen über den Landesbeauftragten für den Datenschutz ausüben. Dies dient der Umsetzung von Artikel 17 Abs. 1 der Richtlinie (EU) 2016/680 und kommt einer deklaratorischen Wiederholung des im Thüringer Datenschutzgesetzes alte Fassung und nun auch in § 8 enthaltenen Grundsatzes gleich, wonach betroffene Personen jederzeit den Landesbeauftragten anrufen können. Satz 2 sieht in Umsetzung von Artikel 17 Abs. 2 der Richtlinie (EU) 2016/680 eine entsprechende Unterrichtung durch den Verantwortlichen vor, die allerdings nicht auf Fälle Anwendung findet, in denen der Verantwortliche nach Absatz 5 berechtigt ist, von einer Information des Antragstellers ganz abzusehen. Satz 3 nimmt den Rechtsgedanken des bisherigen § 13 Abs. 7 ThürDSG a. F. auf. Sätze 4 und 5 bestimmen den Mindestinhalt der Unterrichtung durch den Landesbeauftragten zu seiner Überprüfung; hier wird Artikel 17 Abs. 3 Satz 1 der Richtlinie (EU) 2016/680 umgesetzt und zur Stärkung der Betroffenenrechte in Satz 5 über das von der Richtlinie Geforderte hinausgegangen, indem die Mitteilung die Information enthalten darf, ob datenschutzrechtliche Verstöße festgestellt wurden, mithin die Auskunftsverweigerung oder teilweise die Einschränkung der Auskunft rechtmäßig war. Satz 6 sieht zur Sicherstellung laufender Ermittlungen im weitesten Sinne und zum Schutz von Rechtsgütern vor, dass die Mitteilung des Landesbeauftragten für den Datenschutz ohne Zustimmung durch den Verantwortlichen keine Rückschlüsse auf dessen Erkenntnisstand zulassen darf. Satz 7 setzt Artikel 17 Abs. 3 Satz 2 der Richtlinie (EU) 2016/680 um.

Zu Absatz 7:

Absatz 7 setzt Artikel 15 Abs. 4 der Richtlinie (EU) 2016/680 um.

Zu § 43

Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung (Artikel 16 der Richtlinie (EU) 2016/680)

In § 43 werden die Betroffenenrechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung und deren Ausnahmen zusammengeführt. Dies dient der Umsetzung von Artikel 16 der Richtlinie (EU) 2016/680 in seiner Ausformung als Betroffenenrecht.

Zu Absatz 1:

Absatz 1 betrifft das Recht auf Berichtigung unrichtiger bzw. auf Vervollständigung unvollständiger Daten. Hier wird Artikel 16 Abs. 1 der Richtlinie (EU) 2016/680 umgesetzt. In Satz 2 wird ein in Erwägungsgrund 47 der Richtlinie (EU) 2016/680 enthaltener Gedanke aufgenommen, wonach zur Vorbeugung massenhafter und nicht erfolgversprechender Anträge klargestellt wird, dass sich die Berichtigung auf die betroffene Person bezogene Tatsachen bezieht und nicht etwa auf den Inhalt von Zeugenaussagen; Gleiches gilt etwa für polizeifachliche Bewertungen. In Satz 3 wird Artikel 16 Abs. 3 Satz 1 Buchst. a der Richtlinie (EU) 2016/680 umgesetzt. Zwar sieht der Richtlinienentwurf im beschriebenen Fall die Verarbeitungseinschränkung als Alternative zur Löschung vor. Da die Richtlinie allerdings im Fall der Verarbeitung unrichtiger Daten deren Berichtigung, aber nicht deren Löschung vorsieht, wird der in der Richtlinie beschriebene Sachverhalt systematisch korrekt in Absatz 1 verortet, indem für Fälle, in denen nach Bestreiten der Richtigkeit der Daten deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, an die Stelle der Berichtigung eine Verarbeitungseinschränkung tritt. Für das Bestreiten der Richtigkeit der beim Verantwortlichen verarbeiteten Daten durch die betroffene Person reicht die reine Behauptung der Unrichtigkeit nicht aus; vielmehr müssen die Zweifel an der Unrichtigkeit durch Beibringung geeigneter Tatsachen substantiiert werden. Dies dient dem Schutz der polizeifachlichen Arbeit und der Vermeidung unverhältnismäßigen Prüfaufwands.

Zu Absatz 2:

Absatz 2 regelt das Betroffenenrecht auf Löschung und dient der Umsetzung von Artikel 16 Abs. 2 der Richtlinie (EU) 2016/680, in dem sowohl die unabhängig von der Geltendmachung des Betroffenenrechts durch die betroffene Person bestehende Löschungspflicht des Verantwortlichen als auch das entsprechende Betroffenenrecht angesprochen sind.

Zu Absatz 3:

Absatz 3 verweist in Bezug auf die Voraussetzungen, unter denen an die Stelle einer Löschung nach Absatz 2 eine Verarbeitungseinschränkung treten kann sowie hinsichtlich der Verpflichtung zur Meldung der Berichtigung an Stellen, von denen die unrichtigen Daten stammen, auf eine entsprechende Anwendung von § 35 Abs. 3 beziehungsweise 4.

Zu Absatz 4 und 5:

Absatz 4 dient der Umsetzung von Artikel 16 Abs. 4 der Richtlinie (EU) 2016/680 und betrifft das zur Anwendung kommende Verfahren, wenn der Verantwortliche einem Antrag auf Berichtigung oder Löschung nicht oder nur eingeschränkt nachkommt. Die Bestimmung ist § 42 Abs. 5 nachgebildet; folgerichtig wird - so auch in Absatz 5 - weitgehend auf die entsprechenden Bestimmungen in § 42 zur vollständigen oder teilweisen Einschränkung des Auskunftsrechts verwiesen.

Zu § 44

Verfahren für die Ausübung der Rechte der betroffenen Person (Artikel 12 Abs. 1 und 3 bis 5 der Richtlinie (EU) 2016/680)

In § 44 werden Elemente des Artikels 12 der Richtlinie (EU) 2016/680 umgesetzt. Wenngleich es Artikel 12 Abs. 5 der Richtlinie (EU) 2016/680 dem Verantwortlichen in begründeten Zweifelsfällen ermöglicht, zusätzliche Informationen oder Nachweise zur Identitätsklärung anzufordern, ist hierdurch keine Änderung der bisherigen verbreiteten Praxis angezeigt, den Nachweis der Identität auch weiterhin als Grundvoraussetzung für die Antragsstellung anzusehen.

Zu § 45**Schadensersatz (Artikel 56 der Richtlinie (EU) 2016/680)**

Zu Absatz 1:

Die Bestimmung setzt Artikel 56 der Richtlinie (EU) 2016/680 um, in dem es in Absatz 1 Satz 1 einen Schadensersatzanspruch der betroffenen Person wegen einer rechtswidrigen Verarbeitung seiner personenbezogenen Daten statuiert. Der Ersatzanspruch richtet sich wahlweise gegen den Verantwortlichen oder seinen Rechtsträger. Eine Festlegung des im Einzelfall konkreten Ersatzpflichtigen im jeweiligen Fachrecht bleibt davon unberührt. Absatz 1 Satz 2 regelt den Wegfall der Ersatzpflicht.

Zu Absatz 2:

Absatz 2 bestimmt, dass wegen immaterieller Schäden eine Geldentschädigung verlangt werden kann.

Zu Absatz 3:

Absatz 3 bestimmt für den Fall, dass nicht feststellbar ist, welcher von mehreren Verantwortlichen den Schaden verursacht hat, jeder Verantwortliche oder sein Rechtsträger für den Schaden haftet.

Zu Absatz 4:

Absatz 4 regelt, dass ein Mitverschulden der betroffenen Person bei der Schadensentstehung zu berücksichtigen ist und erklärt hierfür die Bestimmung des § 254 BGB für entsprechend anwendbar.

Zu Absatz 5:

Absatz 5 regelt die Verjährungsfrist für Schadensersatzansprüche und erklärt die für unerlaubte Handlungen geltenden Verjährungsbestimmungen des BGB für entsprechend anwendbar.

Zum Dritten Unterabschnitt**Pflichten der Verantwortlichen und Auftragsverarbeiter****Zu § 46****Pflichten des Verantwortlichen (Artikel 20 der Richtlinie (EU) 2016/680)**

Zu Absatz 1:

Durch § 46 soll Artikel 20 der Richtlinie (EU) 2016/680 umgesetzt werden, der generische Anforderungen an die datenschutzfreundliche Gestaltung von Datenverarbeitungssystemen (Privacy by Design) und die Implementierung datenschutzfreundlicher Grundeinstellungen (Privacy by Default) formuliert. Der Norm liegt der Gedanke zugrunde, dass der Aufwand zur Verfolgung der hier formulierten Ziele und Anforderungen im Sinne effizienten Mitteleinsatzes in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen sollte.

Zu Absatz 2:

Die in Absatz 2 angesprochene Anforderung, die automatisierte umfassende Zugänglichmachung personenbezogener Daten zu verhindern, mündet letztlich in die Anforderung, eine solche Zugänglichmachung stets durch menschliches Zutun einer Prüfung zu unterziehen.

Zu § 47**Gemeinsam Verantwortliche (Artikel 21 der Richtlinie (EU) 2016/680)**

§ 47 dient der Umsetzung von Artikel 21 der Richtlinie (EU) 2016/680. Zur beispielhaften Konkretisierung der infrage kommenden Fälle wird zudem eine Formulierung aus dem bisherigen § 5 Abs. 3 ThürDSG a. F. übernommen.

Zu § 48**Auftragsverarbeitung (Artikel 22 der Richtlinie (EU) 2016/680)**

§ 48 dient der Umsetzung von Artikel 22 der Richtlinie (EU) 2016/680 und stellt Anforderungen auf, wenn der Verantwortliche Auftragsverarbeitungsverhältnisse eingehen will. Gleichzeitig werden Elemente des bisherigen § 8 ThürDSG a. F. überführt. Am bisherigen Regelungsansatz, wonach der Verantwortliche für die Datenübermittlung an den Auftragsverarbeiter keiner gesonderten Rechtsgrundlage bedarf, ändert sich durch die Richtlinienumsetzung nichts.

Zu Absatz 1:

Absatz 1 greift die Regelung des bisherigen § 8 Abs. 1 ThürDSG a. F. auf.

Zu Absatz 2:

Absatz 2 beschreibt an den Auftragsverarbeiter zu stellende Anforderungen und setzt Artikel 22 Abs. 1 der Richtlinie (EU) 2016/680 um.

Zu Absatz 3:

In Absatz 3 werden Voraussetzungen für die Eingehung von Unterauftragsverarbeitungsverhältnissen normiert und dadurch Artikel 22 Abs. 2 der Richtlinie (EU) 2016/680 umgesetzt.

Zu Absatz 4:

In Absatz 4 wird in Übernahme von Elementen aus Artikel 28 Abs. 4 der Verordnung (EU) 2016/679 die Überführung von den Auftragsverarbeitern betreffenden Pflichten auf einen Unterauftragnehmer thematisiert.

Zu Absatz 5:

In Absatz 5 wird die in Artikel 28 Abs. 5 der Verordnung (EU) 2016/679 bestimmte Möglichkeit aufgenommen, dass der Umstand der Einhaltung genehmigter Verhaltensregeln nach Artikel 40 der Verordnung (EU) 2016/679 oder eines genehmigten Zertifizierungsverfahrens nach Artikel 42 der Verordnung (EU) 2016/679 durch den Auftragsverarbeiter zum Nachweis des Vorliegens geeigneter Garantien im Sinne der vorstehenden Absätze herangezogen werden kann.

Zu Absatz 6:

In Absatz 6 werden die erforderlichen Inhalte einer der Auftragsverarbeitung zugrunde liegenden Vereinbarung niedergelegt. Diese Inhalte sind sowohl Artikel 22 Abs. 3 der Richtlinie (EU) 2016/680, Artikel 28 Abs. 3 der Verordnung (EU) 2016/679 als auch der bisherigen Bestimmung des § 8 Abs. 2 und 3 ThürDSG a. F. entnommen.

Zu Absatz 7:

Absatz 7 trifft in Umsetzung von Artikel 22 Abs. 4 der Richtlinie (EU) 2016/680 Aussagen zur Form der Vereinbarung.

Zu Absatz 8:

Absatz 8 dient der Umsetzung von Artikel 22 Abs. 5 der Richtlinie (EU) 2016/680.

Zu § 49**(Verarbeitung auf Weisung, Datengeheimnis (Artikel 23 der Richtlinie (EU) 2016/680))**

Zu Absatz 1:

Absatz 1 setzt Artikel 23 der Richtlinie (EU) 2016/680 um und übernimmt Elemente des § 6 ThürDSG a. F.

Zu Absatz 2:

Absatz 2 greift die bisherige Bestimmung des § 6 ThürDSG a. F. auf.

Zu § 50

Verzeichnis von Verarbeitungstätigkeiten (Artikel 24 der Richtlinie (EU) 2016/680)

§ 50 dient der Umsetzung von Artikel 24 der Richtlinie (EU) 2016/680 und verpflichtet den Verantwortlichen zur Führung eines Verzeichnisses über bei ihm durchgeführte Kategorien von Datenverarbeitungstätigkeiten. Dieses Verzeichnis dient vor allem dem Landesbeauftragten für den Datenschutz dazu, einen Überblick über die beim Verantwortlichen durchgeführten Datenverarbeitungen zu erhalten. Das Zusammenspiel von Anhörung des Landesbeauftragten (§ 53), Einsicht in das Verzeichnis (§ 50 Abs. 4) und Zurverfügungstellung von Protokolldaten (§ 51 Abs. 5) gewährt dem Landesbeauftragten ein umfassendes Bild über die beim Verantwortlichen durchgeführten Datenverarbeitungen. Dies ermöglicht es ihm, seine Aufgaben und Befugnisse im Hinblick auf den jeweiligen Verantwortlichen zielgerichtet, effizient und verhältnismäßig auszurichten und zu nutzen. Die Beteiligung des Landesbeauftragten wird arrondiert und ergänzt durch die interne Beratungs- und Kontrolltätigkeit des Datenschutzbeauftragten nach § 15. Das durch § 50 eingeführte Verzeichnis ist von dem System der Errichtungsanordnungen für Dateien zu unterscheiden und muss diese fachgesetzlich in einigen Bereichen vorgesehene Möglichkeit der Vorbereitung, Planung und Vorprüfung vorgesehener Verarbeitungen nicht enthalten.

Zu Absatz 1:

In Absatz 1 werden die in das Verzeichnis aufzunehmenden Angaben benannt. Die Begrifflichkeit "Kategorien von Datenverarbeitungstätigkeiten" stellt hierbei klar, dass sich das Verzeichnis nicht auf einzelne Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenz- und kategorisierbare Teile der beim Verantwortlichen durchgeführten Datenverarbeitungen bezieht. Es kann sich anbieten, die nach Satz 1 Nummer 2 aufzunehmenden Angaben zu den Zwecken der Verarbeitung an den gesetzlichen Aufgabenzuschreibungen der betreffenden öffentlichen Stelle auszurichten.

Zu Absatz 2:

Absatz 2 verpflichtet den Verantwortlichen, ein Verzeichnis, wenngleich in geringerem Umfang, auch für Verarbeitungen zu führen, wenn er personenbezogene Daten im Auftrag verarbeitet.

Zu Absatz 3:

In Absatz 3 werden Aussagen zur Form des Verzeichnisses getroffen.

Zu Absatz 4:

Nach Absatz 4 wird das Verzeichnis und seine Aktualisierungen dem Landesbeauftragten für den Datenschutz auf Anfrage zur Verfügung gestellt.

Zu § 51

Protokollierung (Artikel 25 der Richtlinie (EU) 2016/680)

Zu Absatz 1:

§ 51 dient der Umsetzung von Artikel 25 der Richtlinie (EU) 2016/680 und enthält in Absatz 1 eine umfassende Pflicht des Verantwortlichen zur Protokollierung der unter seiner Verantwortung durchgeführten Datenverarbeitungen.

Zu Absatz 2:

Absatz 2 enthält konkrete Vorgaben an den Inhalt der Protokolle.

Zu Absatz 3:

Absatz 3 schränkt die Verwendung ein, wobei von der durch die Richtlinie (EU) 2016/680 eröffneten Möglichkeit, die Protokolldaten über die Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit hinaus auch im Zusammenhang mit der Verhütung oder Verfolgung von Straftaten zu verwenden, Gebrauch gemacht wird.

Zu Absatz 4:

In Absatz 4 wird eine Löschfrist für die Protokolldaten generiert.

Zu Absatz 5:

In Absatz 5 wird festgelegt, dass die Protokolle dem Landesbeauftragten für den Datenschutz zum Zwecke der Datenschutzkontrolle zur Verfügung stehen müssen.

Zu § 52

Durchführung einer Datenschutz-Folgenabschätzung (Artikel 27 der Richtlinie (EU) 2016/680)

§ 52 dient der Umsetzung von Artikel 27 der Richtlinie (EU) 2016/680. Die Datenschutz-Folgenabschätzung ist ein zentrales Element der strukturellen Stärkung des Datenschutzes. Die Voraussetzungen zur Durchführung einer Datenschutz-Folgenabschätzung können nur in grundsätzlichen Zügen gesetzlich konkret ausgestaltet werden. So lässt sich dennoch feststellen, dass hinsichtlich des Umfangs der Verarbeitung nicht eine Einzelverarbeitung, sondern lediglich die Verwendung maßgeblicher Systeme und Verfahren zur Verarbeitung personenbezogener Daten mithilfe einer Datenschutz-Folgenabschätzung vorab in den Blick genommen werden muss. Insoweit lässt sich - abseits der prozeduralen Verbindung - eine Vergleichbarkeit mit den Voraussetzungen der Durchführung einer Anhörung des Landesbeauftragten für den Datenschutz begründen. Kriterien für die Entscheidung, ob die vorgesehene Verarbeitung qualitativ erhöhte Gefahren für die Rechtsgüter der betroffenen Person in sich birgt, können beispielsweise der Kreis der betroffenen Personen, die Art der zur Datenerhebung eingesetzten Mittel oder der Kreis der zugriffsberechtigten Personen, mithin die Eingriffsintensität der mit der Verarbeitung verbundenen Maßnahmen im Sinne einer Gesamtwürdigung sein.

Zu Absatz 1:

Die Konkretisierung der in Absatz 1 genannten Voraussetzungen obliegt letztlich der Praxis. Bei diesem Konkretisierungsvorgang wird allerdings zu beachten sein, dass die entstehenden Aufwände angemessen und beherrschbar bleiben müssen. Ferner ist festzuhalten, dass das Erfordernis einer Datenschutz-Folgenabschätzung nur für neue Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden Verarbeitungssystemen gilt.

Zu Absatz 2:

Absatz 2 nimmt Artikel 35 Abs. 1 Nr. 2 der Verordnung (EU) 2016/679 auf.

Zu Absatz 3:

Absatz 3 nimmt Artikel 35 Abs. 2 der Verordnung (EU) 2016/679 auf.

Zu Absatz 4:

Absatz 4 legt den Inhalt der Datenschutz-Folgenabschätzung fest und konkretisiert die in Artikel 27 Abs. 2 der Richtlinie (EU) 2016/680 enthaltenen allgemeinen Angaben durch Übernahme der Angaben aus Artikel 35 Abs. 7 der Verordnung (EU) 2016/679.

Zu Absatz 5:

Absatz 5 nimmt Artikel 35 Abs. 11 der Verordnung (EU) 2016/679 auf.

Zu § 53

Anhörung des Landesbeauftragten für den Datenschutz (Artikel 28 der Richtlinie (EU) 2016/680)

§ 53 dient der Umsetzung von Artikel 28 der Richtlinie (EU) 2016/680. Die Vorkonsultation - hier als Anhörung bezeichnet - des Landesbeauftragten für den Datenschutz dient der datenschutzrechtlichen Absicherung in Bezug auf beabsichtigte Verarbeitungen in neu anzulegenden Dateisystemen, die ein erhöhtes Gefährdungspotential für Rechtsgüter der betroffenen Personen in sich bergen. Insofern besteht eine enge inhaltliche Verbindung zum Instrument der Datenschutz-Folgenabschätzung (§ 52). Prozedural wird diese Verbindung dadurch hergestellt, dass nach Absatz 1 Nummer 1 eine Anhörung durchzuführen ist, wenn im Ergebnis einer Datenschutz-Folgenabschätzung eine erhöhte Gefährdung angenommen wird und der Verantwortliche hierauf nicht mit Maßnahmen zur Gefährdungsminimierung reagiert.

Der Umfang der dem Landesbeauftragten vorzulegenden Unterlagen wird in Absatz 2 durch Zusammenführung der Vorgaben aus Artikel 28 Abs. 4 der Richtlinie (EU) 2016/680 und aus Artikel 36 Abs. 3 der Verordnung (EU) 2016/679 angeglichen. Artikel 28 der Richtlinie (EU) 2016/680 knüpft an die Einleitung der Konsultation an, setzt aber nicht voraus, dass diese zwingend abgeschlossen sein muss, bevor personenbezogene Daten entsprechend verarbeitet werden. Zwar wird man im Regelfall den Abschluss der Konsultation im Interesse der betroffenen Personen abwarten. Im Ausnahmefall können jedoch Abweichungen geboten sein. Die in Absatz 4 vorgesehene Eilfallregelung trägt solchen operativen und (polizei-)fachlichen Erfordernissen in Abweichung von Absatz 3 Satz 1 Rechnung. Die Nutzung der Eilfallregelung entbindet den Verantwortlichen gleichwohl nicht davon, die Empfehlungen des Landesbeauftragten nach pflichtgemäßem Ermessen zu prüfen und die Verarbeitung gegebenenfalls daraufhin anzupassen. Weiterhin begrenzt die Eilfallregelung nicht die dem Landesbeauftragten zur Verfügung stehenden Befugnisse.

Zum Vierten Unterabschnitt Datensicherheit

Zu § 54

Anforderungen an die Sicherheit der Datenverarbeitung (Artikel 29 der Richtlinie (EU) 2016/680)

§ 54 dient der Umsetzung von Artikel 29 der Richtlinie (EU) 2016/680. Er verpflichtet den Verantwortlichen dazu, erforderliche technisch-organisatorische Maßnahmen zu treffen. Gleichzeitig wird klargestellt, dass die Ausgestaltung der Maßnahmen das Ergebnis eines Abwägungsprozesses sein soll, in den insbesondere der Stand der verfügbaren Technik, die entstehenden Kosten, die näheren Umstände der Verarbeitung und die in Aussicht zu nehmende Gefährdung für die Rechtsgüter der betroffenen Person einzustellen sind. Weiterhin wird klarstellend geregelt, dass bei der Festlegung der technisch-organisatorischen Maßnahmen

die einschlägigen Standards und Empfehlungen, insbesondere technische Richtlinien des Bundesamts für Sicherheit in der Informationstechnik, zu berücksichtigen sind.

Zu Absatz 1:

Absatz 1 liegt der schon in der bisherigen Bestimmung des § 9 Abs. 1 Satz 2 ThürDSG a. F. enthaltene Gedanke zugrunde, wonach die Erforderlichkeit der Maßnahmen daran zu bemessen ist, ob ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht.

Zu Absatz 2:

In Absatz 2 werden Inhalte aus Artikel 32 Abs. 1 Buchst. a bis c der Verordnung (EU) 2016/679 übernommen.

Zu Absatz 3:

Absatz 3 dient der Umsetzung von Artikel 29 Abs. 2 der Richtlinie (EU) 2016/680 und übernimmt dabei Inhalte der bereits in § 9 Abs. 2 ThürDSG a. F. enthaltenen Bestimmung. Er benennt die Ziele, die im Hinblick auf automatisierte Verarbeitungen durch die Etablierung geeigneter technisch-organisatorischer Maßnahmen verfolgt und erreicht werden sollen.

Zu § 55

Meldung von Verletzungen des Schutzes personenbezogener Daten an den Landesbeauftragten für den Datenschutz (Artikel 30 der Richtlinie (EU) 2016/680)

Zu Absatz 1 bis 6:

§ 55 dient der Umsetzung von Artikel 30 der Richtlinie (EU) 2016/680 und legt den Umfang und die Modalitäten der Meldung von "Verletzungen des Schutzes personenbezogener Daten" nach § 32 Nr. 10 an den Landesbeauftragten für den Datenschutz fest. Ansatzpunkte der Meldung sind, wie sich auch aus der systematischen Stellung der Bestimmung im Bereich Sicherheit der Verarbeitung ergibt, Vorfälle wie etwa Datenabflüsse. Die in Absatz 5 geforderte Dokumentation muss in Qualität und Quantität so beschaffen sein, dass sie dem Landesbeauftragten die Überprüfung der Einhaltung der gesetzlichen Vorgaben ermöglicht.

Zu Absatz 7:

Absatz 7 stellt klar, dass die in § 56 enthaltene Meldepflicht an den Landesbeauftragten andere Meldepflichten nicht ausschließt beziehungsweise diesen nicht vorgeht.

Zu § 56

Benachrichtigung der betroffenen Person bei Verletzungen des Schutzes personenbezogener Daten (Artikel 31 der Richtlinie (EU) 2016/680)

§ 56 setzt Artikel 31 der Richtlinie (EU) 2016/680 um.

Zum Fünften Unterabschnitt

Übermittlung personenbezogener Daten an Drittstaaten oder internationale Organisationen

Zu § 57

Allgemeine Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten und internationale Organisationen (Artikel 35 und 36 der Richtlinie (EU) 2016/680)

§ 57 dient der Umsetzung von Artikel 35 der Richtlinie (EU) 2016/680 und statuiert Voraussetzungen, die bei jeder Datenübermittlung an Stel-

len in Drittstaaten oder an internationale Organisationen vorliegen müssen. Darüber hinaus enthält die Bestimmung zusätzliche Anforderungen an die Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen - auch an die insbesondere nach den §§ 58 bis 60 erforderliche Abwägungsentscheidung - aufgrund der Rechtsprechung des Bundesverfassungsgerichts (so etwa in BVerfG, Urteil vom 20. April 2016 - 1 BvR 966/09 u. 1 BvR 1140/09). In besonderer Ausprägung dessen fordert Absatz 2 ein Unterbleiben der Übermittlung, wenn im Einzelfall Anlass zur Besorgnis besteht und diese Besorgnis auch nach einer Prüfung durch den Verantwortlichen weiter besteht, dass ein elementaren rechtsstaatlichen Grundsätzen genügender Umgang mit den übermittelten Daten nicht gesichert ist; hierbei ist - unter Übernahme eines Gedankens aus § 14 Absatz 7 Bundeskriminalamtgesetz (BKAG a. F.) - besonders zu berücksichtigen, wenn der Empfänger einen angemessenen Schutz der Daten garantiert.

Zu § 58

Datenübermittlung bei geeigneten Garantien (Artikel 37 der Richtlinie (EU) 2016/680)

Zu Absatz 1:

§ 58 dient der Umsetzung von Artikel 37 der Richtlinie (EU) 2016/680. In § 58 werden § 57 ergänzende Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten, zu denen die Europäische Kommission keinen Angemessenheitsbeschluss nach Artikel 36 gefasst hat, formuliert. Bei solchen Konstellationen kommt dem Verantwortlichen - insbesondere nach § 58 Abs. 1 Nr. 2 - die Aufgabe zu, das Vorliegen geeigneter Garantien für den Schutz personenbezogener Daten beim Empfänger zu beurteilen. Im Zusammenhang mit dem auch hier anwendbaren § 57 Abs. 2 entfaltet der dort erwähnte Gesichtspunkt der Einzelfallgarantie des Empfängerstaats bei der Prüfung des Vorhandenseins geeigneter Garantien besondere Bedeutung.

Zu Absatz 2:

Absatz 2 dient der Umsetzung von Artikel 37 Abs. 3 der Richtlinie (EU) 2016/680 zur Dokumentation der Übermittlungen nach § 58.

Zu Absatz 3:

Absatz 3 dient der Umsetzung von Artikel 37 Abs. 2 der Richtlinie (EU) 2016/680, der die Unterrichtung des Landesbeauftragten für den Datenschutz über Kategorien von Übermittlungen vorsieht, die ohne Vorliegen eines Angemessenheitsbeschlusses der Kommission, aber wegen Bestehens geeigneter Garantien für den Schutz personenbezogener Daten im Drittstaat nach entsprechender Beurteilung durch den übermittelnden Verantwortlichen erfolgen.

Zu § 59

Datenübermittlung ohne Angemessenheitsbeschluss und ohne geeignete Garantien (Artikel 38 Richtlinie (EU) 2016/680)

§ 59 dient der Umsetzung von Artikel 38 der Richtlinie (EU) 2016/680 und regelt Konstellationen, in denen weder ein Angemessenheitsbeschluss der Europäischen Kommission vorliegt noch die in § 58 erwähnten Garantien in Form eines rechtsverbindlichen Instruments oder soweit nach Beurteilung durch den übermittelnden Verantwortlichen bestehen.

Zu § 60**Sonstige Datenübermittlung an Empfänger in Drittstaaten (Artikel 39 der Richtlinie (EU) 2016/680)**

§ 60 dient der Umsetzung von Artikel 39 der Richtlinie (EU) 2016/680. Die hier geregelte Konstellation zeichnet sich dadurch aus, dass der Kreis der möglichen Empfänger über öffentliche Stellen, die im Rahmen der Strafverfolgung tätig sind, hinaus auf sonstige öffentliche Stellen und Private ausgeweitet wird. Abgebildet werden etwa Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister, die notwendigerweise mit der Übermittlung personenbezogener Daten verbunden sind. Für solche Übermittlungen "im besonderen Einzelfall" gelten die in § 60 Abs. 1 genannten strengen Voraussetzungen. In Absatz 3 ist eine verstärkte Zweckbindung der nach § 60 übermittelten Daten vorgesehen.

Zum Vierten Abschnitt**Ordnungswidrigkeiten und Strafbestimmungen****Zu § 61****Ordnungswidrigkeiten und Strafbestimmungen**

§ 61 regelt die Voraussetzungen, unter denen aufgrund eines Verstoßes gegen die Bestimmungen der Verordnung (EU) 2016/679, dieses Gesetzes oder einer datenschützenden Rechtsvorschrift Ordnungswidrigkeiten und Straftaten verfolgt werden können. Dabei ist nach Absatz 1 bis 3 der Landesbeauftragte für die Verfolgung von Ordnungswidrigkeiten, nach Absatz 5 die Staatsanwaltschaft für die Verfolgung von Straftaten zuständig.

Die Norm übernimmt zum Großteil die bisherige Regelung des § 43 ThürDSG a. F. Neu hinzugekommen ist Absatz 6.

Zu Absatz 1 und 2:

In Artikel 83 der Verordnung (EU) 2016/679 sind die Bedingungen und Tatbestände für die Verhängung von Geldbußen gegen den Verantwortlichen und den Auftragsverarbeiter geregelt. Die Verordnung (EU) 2016/679 enthält keine Regelungen zur Verhängung von Geldbußen gegenüber Mitarbeitern des Verantwortlichen. Artikel 84 Abs. 1 der Verordnung (EU) 2016/679 enthält diesbezüglich eine Öffnungsklausel. Danach legen die Mitgliedstaaten der Europäischen Union, "insbesondere für Verstöße, die keiner Geldbuße nach Artikel 83 unterliegen", Bestimmungen über Sanktionen fest.

§ 61 Abs. 1 greift auf der Grundlage dieser Öffnungsklausel die bisherige Regelung des § 43 Abs. 1 ThürDSG a. F. auf, nach der die Verhängung von Geldbußen auch gegenüber Mitarbeitern öffentlicher Stellen möglich ist.

§ 61 Abs. 2 begrenzt die Höhe des Bußgeldes wie bisher auf 50.000 Euro.

Zu Absatz 3:

Absatz 3 stellt unter Strafe, wer eine Datenübermittlung durch unrichtige Angaben erschleicht. Die Bestimmung entspricht der bisherigen Regelung in § 43 Abs. 2 Nr. 1 ThürDSG a. F. Die bisherigen Fälle der unrechtmäßigen Weitergabe von Daten oder Zusammenführen von Einzelangaben sind bereits nach Absatz 1 als Ordnungswidrigkeit eingestuft.

Zu Absatz 4:

Absatz 4 ergänzt die Bestimmung des § 7 Abs. 2 speziell für den Bereich der Ordnungswidrigkeiten. Die Regelungsbefugnis folgt aus Artikel 83 Abs. 7 der Verordnung (EU) 2016/679.

Zu Absatz 5:

Absatz 5 entspricht der bisherigen Bestimmung in § 43 Abs. 3 ThürDSG a. F. Im neuen Datenschutzrecht mit seinen Verweisen auf die Verordnung (EU) 2016/679 und die Richtlinie (EU) 2016/680 ist zu berücksichtigen, dass die Materie determiniert ist durch eine Vielzahl von Rechtsvorschriften auf Europa-, Bundes- und Landesebene. Für die datenverarbeitende Stelle kann daher die rechtstreue Datenverarbeitung mit gewissen Unwägbarkeiten verbunden sein. Dies gilt gerade für die nicht weiter qualifizierten Tatbestände der Absätze 1 und 3. Die Folge einer strafrechtlichen Verantwortlichkeit, die ein über die bloße Rechtsverletzung hinausgehendes eigenständiges Unrecht enthält, ist daher auf qualifizierte Rechtsverstöße beschränkt, die als Handeln gegen Entgelt oder mit besonderer Schädigungsabsicht oder Bereicherungsabsicht in gesteigertem Maße verwerflich sind.

Zu Absatz 6:

Absatz 6 legt gesetzlich fest, dass der Landesbeauftragte für den Datenschutz die für die Verfolgung und Ahndung von Ordnungswidrigkeiten zuständige Stelle ist.

Zum Fünften Abschnitt Orden und Ehrenzeichen, Gnadensachen

Der Fünfte Abschnitt regelt für die Datenverarbeitung zur Verleihung von Orden und Ehrenzeichen sowie für die Entscheidung in Gnadensachen Ausnahmen von den Informations- und Auskunftspflichten. Orden und Ehrenzeichen sowie Gnadensachen fallen nicht in den Anwendungsbereich der Verordnung (EU) 2016/679. Nach § 2 Abs. 5 sind jedoch die Bestimmungen der Verordnung (EU) 2016/679 entsprechend anwendbar. Ausnahmen von den Auskunftspflichten waren für diese Fälle bereits nach bisherigem Recht normiert. Durch die Bestimmungen im Fünften Abschnitt soll den besonderen Belangen des Datenschutzes in diesem Bereich Rechnung getragen werden. Da es sich um Datenverarbeitungen außerhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 handelt, wurden sie in einem eigenen Abschnitt zusammengefasst. Im Übrigen gelten aber wegen § 2 Abs. 5 die Bestimmungen dieses Gesetz und die Verordnung (EU) 2016/679, so dass sichergestellt ist, dass die Anforderungen der Verordnung (EU) 2016/679 in Bezug auf die Grundsätze der Verarbeitung und den technischen und organisatorischen Datenschutz eingehalten werden und die Datenverarbeitung der Kontrolle durch den Landesbeauftragten unterliegt.

Zu § 62 Orden und Ehrenzeichen

§ 62 regelt die Ausnahmen von den Informations- und Auskunftspflichten des Verantwortlichen im Falle der Datenverarbeitung zur Entscheidung über Orden und Ehrenzeichen. Es handelt sich bei den zu diesen Zwecken gespeicherten Daten beispielsweise um die Daten von Referenzpersonen, über welche die betroffene Person keine Auskunft erhalten soll, wenn dies für die Referenzpersonen nachteilige Folgen haben kann. Die Umstände, die zu einer positiven oder negativen Entscheidung führen, sind oft zu sensibel und berühren die Integrität der beteiligten Personen, so dass keine Offenlegungspflicht in diesen Fällen zu verlangen ist.

Bereits in der bisherigen Regelung des § 13 Abs. 5 Nr. 4 ThürDSG a. F. wurde eine Ausnahme von den Auskunftspflichten des Verantwortlichen normiert, der Regelungsinhalt wurde auf die Informationsrechte der be-

troffenen Person erweitert, um den Geheimhaltungsbedürfnissen der verantwortlichen staatlichen Stellen als öffentliches Interesse umfassend gerecht zu werden.

Zu § 63 Gnadensachen

Durch § 63 wird die Ausnahme von der Informations- und Auskunftspflicht des Verantwortlichen nach § 62 des Gesetzes bei der Datenverarbeitung zur Entscheidung in Gnadensachen für entsprechend anwendbar erklärt.

Zum Sechsten Abschnitt Übergangs- und Schlussbestimmungen

Zu § 64 Übergangsbestimmungen

Zu Absatz 1:

Da sich hinsichtlich der Dauer der Amtszeit des Landesbeauftragten für den Datenschutz keine Änderungen gegenüber der bisherigen Rechtslage ergeben, berechnet diese sich nach dem Zeitpunkt der Ernennung und wird durch das Inkrafttreten des neuen Gesetzes nicht berührt. Die Möglichkeit zur Wiederwahl, welche sowohl nach bisherigem Recht als auch nach diesem Gesetz besteht, ist verbraucht, wenn der Landesbeauftragte bereits vor dem 25. Mai 2018 in seinem Amt wiedergewählt worden ist. Zudem enthält Absatz 1 eine Übergangsbestimmung für den bei Inkrafttreten dieses Gesetzes gewählten und ernannten Landesbeauftragten für den Datenschutz hinsichtlich des Ruhens seines Ruhegehaltsanspruchs.

Zu Absatz 2:

Der bei Inkrafttreten dieses Gesetzes nach § 35 ThürDSG a. F. gewählte und ernannte Landesbeauftragte für den Datenschutz gilt nach Absatz 2 auch als nach diesem Gesetz zu bestimmende Aufsichtsbehörde.

Zu Absatz 3:

Absatz 3 bestimmt, dass der erste Jahresbericht nach neuer Rechtslage bis zum 25. Mai 2018 die bisherige Rechtslage, also das Thüringer Datenschutzgesetz alte Fassung zu berücksichtigen hat.

Zu Absatz 4:

Absatz 4 dient der Umsetzung von Artikel 63 Abs. 2 der Richtlinie (EU) 2016/680.

Zu § 65 Gleichstellungsbestimmung

§ 65 enthält die Gleichstellungsbestimmung.

Zu Artikel 2 Änderung des Thüringer Gesetzes über das Verfahren bei Bürgerantrag, Volksbegehren und Volksentscheid

Der Gesetzestext wird redaktionell an Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016,

S. 1; L 314 vom 22.11.2016, S. 72) angepasst. Der bisher verwendete Begriff "Nutzen" wird von dem in der Verordnung (EU) 2016/679 verbindlich definierten Oberbegriff "Verarbeitung" mit umfasst.

Zu Artikel 3 Änderung des Ordnungsbehördengesetzes

Zu Nummer 1

Absatz 1:

Im Einleitungssatz zu § 26 des Ordnungsbehördengesetzes der bisherigen Fassung wurde nur die Geltung des Thüringer Datenschutzgesetzes (ThürDSG) in der jeweils geltenden Fassung genannt. Nunmehr ist durch Absatz 1 zusätzlich die Geltung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) zu berücksichtigen, die deshalb in Absatz 1 mit aufgenommen wird. Die Verordnung (EU) 2016/679 kommt in solchen Fällen zur Anwendung, in denen die Ordnungsbehörde nicht zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung tätig wird, zum Beispiel zum Schutz privater Rechte (§ 2 Abs. 2 OBG). Soweit die Ordnungsbehörden jedoch zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung tätig werden, bestimmt sich das dabei zu beachtende europäische Datenschutzrecht nach der Richtlinie (EU) 2016/680, die in Thüringen vor allem durch das Thüringer Datenschutzrecht umgesetzt wird.

Die nachfolgenden Maßgaben beziehen sich nur auf das Thüringer Datenschutzgesetz; die Bestimmungen der Verordnung (EU) 679/2016 werden hierdurch nicht berührt.

Zu Absatz 2 und 3:

Die Absätze 2 und 3 des § 26 des Ordnungsbehördengesetzes werden inhaltlich unverändert übernommen und entsprechen § 26 Nr. 1 und 2 der bisher geltenden Fassung. Bei § 26 Abs. 2 handelt es sich um eine spezielle Form der Datenverarbeitung nach den §§ 31, 33 des ThürDSG n. F. Ergänzend erfolgt eine redaktionelle Anpassung an die neue Rechtschreibung. § 26 Absatz 3 wird durch die Änderung des Datenschutzrechts nicht berührt.

Zu Absatz 4

Absatz 4 des § 26 des Ordnungsbehördengesetzes wird ebenfalls redaktionell angepasst und entspricht § 26 Nr. 3 der bisher geltenden Fassung. Der Anspruch auf Berichtigung unrichtiger Daten sowie die Unterrichtung bei regelmäßiger Datenübermittlung nach der bisherigen Fassung des Thüringer Datenschutzgesetzes ergeben sich zukünftig je nach Kontext der Datenverarbeitung aus den §§ 35 und 43 ThürDSG n. F. oder unmittelbar aus den Artikeln 16 und 19 der Verordnung (EU) 2016/679.

Die bisherige Nummer 4 des § 26 wird gestrichen. Das Freigabeverfahren nach § 34 Abs. 2 des bisherigen Thüringer Datenschutzgesetzes beim erstmaligen Einsatz von automatisierten Verfahren und wesentlichen Verfahrensänderungen ist infolge der Anpassung an die Verordnung (EU) 2016/679 und die Umsetzung der Richtlinie (EU) 2016/680 entfallen. Die Gesamtverantwortung des Verantwortlichen ergibt sich nunmehr je nach Kontext der Datenverarbeitung aus Artikel 5 Abs. 2 sowie Kapitel IV der Verordnung (EU) 2016/679 beziehungsweise aus dem Dritten Abschnitt, Dritter und Vierter Unterabschnitt des Thüringer Datenschutz-

gesetzes. Der Standard für den Schutz personenbezogener Daten wird hierdurch nicht verschlechtert. Stattdessen werden die Sicherstellung des Datenschutzes und der Schutz der Rechte und Freiheiten natürlicher Personen durch eine Reihe neuer Maßnahmen sichergestellt: Der Verantwortliche hat Art, Umfang, Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen abzuwägen und auf dieser Grundlage geeignete technische und organisatorische Maßnahmen zu treffen (Artikel 24, 32 der Verordnung (EU) 2016/679, § 54 ThürDSG). Diese sind in einem Verzeichnis aller Verarbeitungstätigkeiten sowie auch innerhalb der verantwortlichen Stelle zu dokumentieren (§§ 50, 51 ThürDSG, Artikel 30 der Verordnung (EU) 2016/679). Darüber hinaus hat der Verantwortliche den Datenschutz durch Technikgestaltung sowie datenschutzfreundliche Voreinstellungen sicherzustellen (Artikel 25 der Verordnung (EU) 2016/679, § 46 ThürDSG). Hat eine Form der Verarbeitung 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 ist eine Datenschutz-Folgenabschätzung durchzuführen sowie gegebenenfalls der Landesbeauftragte für den Datenschutz zu konsultieren (Artikel 35, 36 der Verordnung (EU) 2016/679, §§ 52, 53 ThürDSG). Bei sämtlichen genannten Maßnahmen ist zudem der behördeninterne Datenschutzbeauftragte frühzeitig zu beteiligen. Insgesamt gesehen bedarf es daher im Geltungsbereich des Ordnungsbehördengesetzes keines gesonderten Freigabeverfahrens mehr.

Zu Absatz 5:

Sofern Ordnungsbehörden im Rahmen der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung tätig werden, wird durch Ziffer 4 Artikel 5 der Richtlinie (EU) 2016/680 konkret ausgestaltet.

Zu Nummer 2

Es handelt sich um eine redaktionelle Anpassung infolge der Änderung der Überschrift des § 26.

Zu Artikel 4 Änderung des Polizeiaufgabengesetzes

Zu Nummer 1 (§ 12)

In § 12 Abs. 1 wird der Verweis auf die Bestimmungen der §§ 13 bis 47 redaktionell geändert und es wird nunmehr nur noch auf die Bestimmungen der §§ 13 bis 44 verwiesen. Die Anpassung des Verweises geht auf die inhaltliche Neufassung der Bestimmung des § 45 und die Aufhebung der Bestimmungen der §§ 46 und 47 zurück.

Zu Nummer 2 (§ 25 Abs. 2)

Es handelt sich um eine redaktionelle Anpassung.

Zu Nummer 3 (§ 31)

Der neue § 31 ist das Ergebnis der Umsetzung von Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) und der Vorga-

ben der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) im novellierten Thüringer Datenschutzgesetz (ThürDSG).

§ 31 wird neu gefasst. Im Zuge der Neufassung wird die Paragrafenüberschrift dem neuen Regelungsinhalt angepasst. § 31 n. F. sieht vor, dass die Polizei personenbezogene Daten unter den Voraussetzungen der Bestimmungen des Polizeiaufgabengesetzes in Verbindung mit den Bestimmungen des Ersten und Dritten Abschnitts des novellierten Thüringer Datenschutzgesetzes verarbeiten kann.

Mit der Neufassung des Thüringer Datenschutzgesetzes im Rahmen der oben genannten Umsetzung der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 in nationales Recht hat sich der Thüringer Gesetzgeber entschieden, im Zweiten Abschnitt des Thüringer Datenschutzgesetzes die dem Landesgesetzgeber durch Öffnungsklauseln in der Verordnung (EU) 2016/679 eröffneten Spielraum durch nationale Regelungen auszufüllen. Im Dritten Abschnitt hat der Landesgesetzgeber die Richtlinie (EU) 2016/680 umgesetzt. Nachdem danach für Sicherheitsbehörden vorgesehene besondere Datenschutzregelungen der Richtlinie (EU) 2016/680 bereits in erheblichem Umfang im Dritten Abschnitt des novellierten Thüringer Datenschutzgesetzes umgesetzt worden sind, erübrigt sich eine umfangreiche parallele Umsetzung der Richtlinie (EU) 2016/680 im Polizeiaufgabengesetz. Aus diesem Grund hat sich der Gesetzgeber entschieden, durch den Globalverweis in § 31 auf die Bestimmungen des Ersten und Dritten Abschnitts des novellierten Thüringer Datenschutzgesetzes diese parallel zu den Bestimmungen im Polizeiaufgabengesetz anzuwenden. Diese jeweiligen Regelungen der beiden Gesetze bedingen sich gegenseitig. Dies hat zur Folge, dass im Datenschutzrecht des Polizeiaufgabengesetzes nur noch polizeispezifische Befugnisse enthalten sind und diese durch die Verfahrensregelungen im Ersten und Dritten Abschnitt des novellierten Thüringer Datenschutzgesetzes vervollständigt werden. Aus der Systematik des § 31 wird zugleich deutlich, dass die Verarbeitung personenbezogener Daten zu anderen als vollzugspolizeilichen Zwecken nicht den Bestimmungen des Polizeiaufgabengesetzes unterliegt, sondern hierfür die Verordnung (EU) 2016/679 unmittelbar und in Verbindung mit den Bestimmungen des Ersten und Zweiten Abschnitts des novellierten Thüringer Datenschutzgesetzes gilt.

Die Regelungen der bisherigen Absätze 2 bis 4 a. F. werden aus systematischen Gründen in § 32 Absätze 3 bis 5 n. F. überführt.

Zu Nummer 4 (§ 32)

In § 32 n. F. werden wie bisher die Grundsätze der Datenerhebung geregelt. Neben der redaktionellen Anpassung des Verweises in § 32 Abs. 1 auf die Bestimmungen der §§ 13 bis 47 aufgrund der inhaltlichen Neufassung und Aufhebung von Bestimmungen des Polizeiaufgabengesetzes werden die bisherigen Regelungen um die Absätze 3 bis 5 erweitert. Die Absätze 3 bis 5 enthalten die bisherigen Regelungen über die Grundsätze der Datenerhebung des § 31 Abs. 2 bis 4 a. F.

Zu Nummer 5 (§ 34 Abs. 4)

Absatz 4 Satz 4 wird zum besseren Verständnis sprachlich neu gefasst und sieht vor, dass personenbezogene Daten, die unter Verwendung besonderer Mittel der Datenerhebung erhoben worden sind, unverzüglich zu löschen sind und die Löschung zu protokollieren ist, wenn die Datenerhebung wegen Gefahr im Verzug ohne richterliche Erlaubnis erfolgt ist und ein Richter diese Anordnung nicht nachträglich bestätigt. Eine Änderung der bisherigen Rechtslage geht mit der sprachlichen Neufassung nicht einher.

Zu Nummer 6 (§ 34 a)

Der dem Absatz 5 neu angefügte Satz 4 regelt den Umgang mit personenbezogenen Daten, die wegen Gefahr im Verzug ohne richterliche Anordnung erhoben worden sind und diese Datenerhebung nicht nachträglich richterlich bestätigt wird. Nach bisheriger Rechtslage war gesetzlich nicht ausdrücklich geregelt, wie mit den Daten zu verfahren ist, die wegen Gefahr im Verzug erhoben worden sind, eine richterliche Bestätigung dieser Datenerhebung aber nicht erfolgt ist. Diese Lücke soll mit dem neu angefügten Satz geschlossen werden. Nunmehr wird gesetzlich verankert, dass personenbezogene Daten unverzüglich zu löschen sind und die Löschung zu protokollieren ist, wenn ein Richter nicht nachträglich die Anordnung auf Überwachung der Telekommunikation bestätigt. Gleichzeitig wird durch den Verweis der anderen Datenerhebungsbefugnisnormen in § 34 b Abs. 3 Satz 1 über die Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten sowie in § 34 c Abs. 3 über die Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten auf den § 34 a Abs. 5 und damit auch auf dessen neu eingefügten Satz 4 einheitlich der Umgang mit personenbezogenen Daten geregelt, deren Erhebung nicht richterlich bestätigt wird.

Zu Nummer 7 (§ 36)

§ 36 Abs. 3 wird geändert. Hierzu wird in Absatz 3 Satz 1 Nr. 9 Buchst. c) in Fällen der Wohnraumüberwachung die Benachrichtigungspflicht von "Personen, die die überwachte Wohnung zur Zeit der Durchführung der Maßnahme innehatten oder bewohnten" gestrichen. Die Benachrichtigungspflicht des Bewohners ergibt sich bereits aus der in § 36 Abs. 3 Satz 1 Nr. 9 Buchst. a) PAG bestimmten Benachrichtigungspflicht. Danach ist im Falle einer Wohnraumüberwachung die Person zu benachrichtigen, gegen die sich die Maßnahme richtet. Dies ist der Bewohner des überwachten Wohnraums. Die Wohnraumüberwachungsmaßnahme richtet sich aber auch gleichzeitig gegen den Wohnungsinhaber, der die Wohnung zwar angemietet hat, aber nicht selbst bewohnt. Dessen Wort ist zwar nicht Gegenstand der Wohnraumüberwachung, gleichwohl ist seine Wohnung Gegenstand der Überwachungsmaßnahme.

Zu Nummer 8 (§§ 38 und 39)

Zu § 38

§ 38 a.F. wird aufgehoben. Die bisherigen Regelungen über die Dauer der Datenspeicherung werden aus systematischen Gründen in § 40 Abs. 5 Sätze 1 und 2 n.F. überführt.

Zu § 39

§ 39 a. F. wird ebenfalls aufgehoben. Die Grundsätze über die Zweckbindung personenbezogener Daten ergeben sich aus § 33 des novellierten Thüringer Datenschutzgesetzes. Aufgrund des Globalverweises in § 31 Satz 1 n. F. auf die Bestimmungen des Ersten und Dritten Abschnitts des novellierten Thüringer Datenschutzgesetzes sind eigene Bestimmungen über die Zweckbindung im Fachrecht der Polizei entbehrlich.

Zu Nummer 9 (§§ 40 und 41)

Zu § 40:

§ 40 wird neu gefasst. Systematisch regelt § 40 nach den einzelnen Bestimmungen über die Datenerhebung die Grundsätze der Weiterverarbeitung von Daten.

Zu Absatz 1:

Absatz 1 entspricht inhaltlich weitgehend dem Absatz 1 a. F. und ist terminologisch an die Vorgaben der Richtlinie (EU) 2016/680 angepasst worden.

Zu Absatz 2:

Absatz 2 regelt die Befugnis zur Weiterverarbeitung von personenbezogenen Daten bestimmter Kategorien von Personen. Der bisherige Grundsatz, nach dem im Rahmen der Strafverfolgung gewonnene Informationen durch die Polizei auch zur Gefahrenabwehr genutzt werden dürfen, war bereits in § 40 Abs. 1 Satz 1 a. F. enthalten. Ergänzt wird die bisherige Regelung durch die Aufzählung bestimmter Kategorien von Personen, deren Daten weiterverarbeitet werden können. Diese Aufzählung von Kategorien ist in Artikel 6 der Richtlinie (EU) 2016/680 vorgesehen. Die konkret aufgezählten Kategorien von Personen entsprechen der Regelung in § 18 Abs. 1 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG) vom 1. Juni 2017 (BGBl. I S. 1354) (BKAG-2018). Die Übernahme der dort genannten Kategorien von Personen in das PAG ermöglicht es, Kompatibilität im Hinblick auf den anstehenden Umbau des polizeilichen Datenverbundes sicherzustellen.

Zu Absatz 3:

Absatz 3 benennt weitere Kategorien zur Verarbeitung von personenbezogenen Daten zur Verhütung von Straftaten. Inhaltlich werden die in Artikel 6 Buchst. c) und d) der Richtlinie (EU) 2016/680 genannten Kategorien konkretisiert. Die Ausgestaltung entspricht auch hier inhaltlich der Bestimmung des § 19 Abs. 1 BKAG-2018.

Zu Absatz 4:

Absatz 4 entspricht Absatz 4 a. F. und sieht weiterhin vor, dass personenbezogene Daten auch zur polizeilichen Aus- und Fortbildung genutzt werden können. Absatz 4 stellt die Rechtsgrundlage im Sinne des Artikels 4 Abs. 2 Richtlinie (EU) 2016/680 für eine Zweckänderung personenbezogener Daten dar.

Zu Absatz 5:

In Absatz 5 werden die Vorgaben von Artikel 5 der Richtlinie (EU) 2016/680 über die Fristen für die Speicherung und die Überprüfung für die Notwendigkeit der Speicherung personenbezogener Daten umgesetzt. Absatz 5 entwickelt den nach der derzeitigen Rechtslage bereits

vorhanden Rahmen für die Ausgestaltung der Aussonderungsprüffristen weiter und führt die bisher in § 38 Satz 4 a. F. (Kinder) und § 40 Abs. 2 Satz 2 a. F. (Erwachsene und Jugendliche) mit den in § 3 der Thüringer Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung vom 26. Februar 2000 genannten "Besonderen Prüffristen" (Zeugen, Hinweisgeber etc.) zusammen. Gleichzeitig erfolgt eine Angleichung an die Regelungen in § 77 BKAG-2018 über die Regelungen zu Aussonderungsprüffristen, um Reibungsverluste im künftigen Datenverbund zu minimieren.

Zu Absatz 6:

Mit der Regelung in Absatz 6 wird klargestellt, dass die Speicherung personenbezogener Daten in den polizeilichen Datensystemen dazu dient, die Entwicklung einer betroffenen Person in kriminalistischer Hinsicht über aussagekräftige Zeiträume abzubilden. Dies wäre erschwert oder unmöglich, wenn innerhalb der Frist zu einer Person hinzugespeicherte Daten aufgrund unterschiedlicher Fristabläufe ausgesondert werden müssten.

Zu Absatz 7:

In dem neu eingefügten Absatz 7 ist die Verordnungsermächtigung für Aussonderungsprüffristen geregelt.

Zu § 41:

§ 41 enthält Regelungen zur Übermittlung personenbezogener Daten im innerstaatlichen Bereich. Als Rechtsgrundlage für die Übermittlung personenbezogener Daten im innerstaatlichen Bereich kommt bereits § 33 Abs. 1 und 2 des novellierten Thüringer Datenschutzgesetzes in Betracht. In § 33 Abs. 1 des ThürDSG n. F. ist beispielsweise bestimmt, dass die Verarbeitung personenbezogener Daten zulässig ist, wenn diese Verarbeitung für die Aufgabenerfüllung zu den in § 31 genannten Zwecken (polizeiliche Zwecke) erforderlich ist und keine speziellen Regelungen in anderen Gesetzen vorgehen. Vor dem Hintergrund, dass der Begriff "Verarbeitung" nach § 32 Nr. 2 ThürDSG n. F. auch die Datenübermittlung erfasst, ist eine weitere über § 33 ThürDSG n. F. hinausgehende Regelung zur Datenübermittlung vom Grundsatz her nicht erforderlich. Gleichwohl hat sich der Gesetzgeber aus Gründen der Verständlichkeit und insbesondere zur Erleichterung der Rechtsanwendung dazu entschieden, in § 41 konkrete Datenübermittlungsbefugnisse vorzusehen, die den Regelungen im novellierten Thüringer Datenschutzgesetz vorgehen.

Zu Absatz 1:

In Absatz 1 sind die bisherigen Regelungen des Absatzes 1 a. F. und Absatzes 2 a. F. zusammengeführt worden. Eine inhaltliche Änderung geht mit dieser Zusammenführung nicht einher.

Zu Absatz 2:

In Absatz 2 werden wie bisher die Voraussetzungen geregelt, unter denen die Polizei an andere Behörden, öffentliche oder nicht öffentliche Stellen sowie Einzelpersonen personenbezogene Daten übermitteln kann.

Zu Absatz 3:

In den Absatz 3 n. F. sind die bisherigen Regelungen des Absatzes 7 a. F. zur Datenübermittlung von Behörden und sonstigen öffentlichen Stellen an die Polizei überführt worden.

Zu Absatz 4:

Die Regelungen in Absatz 4 n. F. entsprechen weitgehend den Regelungen in Absatz 5 a. F. Diese sind lediglich an die geänderte Systematik und Struktur des PAG angepasst worden. Zusätzlich ist Absatz 4 um eine weitere Regelung ergänzt worden, nach der die Polizei bei einer Übermittlung personenbezogener Daten dem Empfänger die bestehenden Lösungsverpflichtungen mitzuteilen hat. Durch die Mitteilung der Lösungsverpflichtung wird auch im Falle einer Datenübermittlung ein einheitlicher Schutz personenbezogener Daten gewährleistet. Die Regelungen im bisherigen Absatz 4 a. F. zur Übermittlung personenbezogener Daten an ausländische Stellen wurden aufgehoben und werden nunmehr gesondert in § 41 c n. F. verortet.

Zu Absatz 5:

Der Absatz 5 n. F. entspricht weitgehend dem Absatz 6 a. F. Dieser ist lediglich an die neue Systematik und Struktur des PAG angepasst worden.

Zu Absatz 6:

Die Regelung im Absatz 6 n. F. entspricht der bisherigen Regelung im Absatz 8 a. F.

Zu Absatz 7:

In den neuen Absatz 7 sind die Regelungen des Absatzes 9 a. F. überführt worden. Die Regelungen des Absatzes 7 a. F. sind in Absatz 3 n. F. enthalten.

Die Regelungen der Absätze 8 a. F. und 9 a. F. sind in die Absätze 6 n. F. und 7 n. F. überführt worden.

Zu Nummer 10 (§§ 41 b bis 41 d)

Zu § 41 b

§ 41 b n. F. regelt die Übermittlung personenbezogener Daten an die Mitgliedstaaten der Europäischen Union.

Zu Absatz 1:

Absatz 1 sieht mit der für entsprechend anwendbar erklärten Bestimmung des § 41 über die Datenübermittlung im innerstaatlichen Bereich vor, dass für die Übermittlung personenbezogener Daten an Mitgliedstaaten der Europäischen Union die gleichen Voraussetzungen gelten, wie für die Datenübermittlung im innerstaatlichen Bereich. Diese Gleichsetzung ist bedingt durch die sich stetig vertiefende europäische Integration, die die Europäische Union zu einem gemeinsamen Raum der Freiheit, der Sicherheit und des Rechts gemacht hat. Ein wesentliches Instrument der Sicherheit in der Bundesrepublik Deutschland und der Europäischen Union ist die Gewährleistung eines effektiven und wirksamen polizeilichen Informationsaustauschs zwischen den Sicherheitsbehörden der Mitgliedstaaten der Europäischen Union. Nur durch die intensive grenzübergreifende Zusammenarbeit der europäischen Sicherheitsbehörden bei der Gefahrenabwehr des internationalen Terrorismus und der Straftatenverhütung und -verfolgung können europaweit terroristische Anschläge und Straftaten verhindert, verfolgt und aufgedeckt werden.

Durch Satz 1 Nummer 1 wird die Übermittlung an Behörden, sonstige öffentliche und nichtöffentliche Stellen anderer Mitgliedstaaten der Europäischen Union den Regelungen über die Übermittlung an inländische Stellen gleichgestellt. Auch wird die dieser Gleichstellung wider-

sprechende Differenzierung zwischen Übermittlungen auf Ersuchen und Spontanübermittlungen aufgegeben.

Über Satz 1 Nummer 2 wird klargestellt, dass sich auch Datenübermittlungen an zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedstaaten, die mit Aufgaben der Verhütung und Verfolgung von Straftaten befasst sind, nach Regelungen über die Übermittlung an Polizeibehörden der Mitgliedstaaten nach Satz 1 Nummer 1 in Verbindung mit § 41 richten. Den Regelfall von Übermittlungen nach Satz 1 Nummer 1 stellen Übermittlungen an Polizeibehörden oder sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stellen eines Mitgliedstaates der Europäischen Union dar. Als solche können insbesondere jene Stellen gelten, die von diesem Staat nach Artikel 2 Buchst. a des Rahmenbeschlusses 2006/960/JI des Rates vom 18. Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (ABl. L 386 vom 29.12.2006, S. 89, L 75 vom 15.3.2007, S. 26) benannt wurden.

Zu Absatz 2:

Der neue Absatz 2 Satz 1 hebt den Vorrang des Gesetzes über die internationale Rechtshilfe in Strafsachen für den Rechtshilfeverkehr mit dem Ausland in strafrechtlichen Angelegenheiten hervor. Satz 2 sieht vor, dass die Zulässigkeit der Übermittlung personenbezogener Daten an eine Polizeibehörde oder eine sonstige für die Verhütung und Verfolgung von Straftaten zuständige öffentliche Stelle eines Mitgliedstaates der Europäischen Union auf der Grundlage besonderer völkerrechtlicher Vereinbarungen unberührt bleibt.

Zu Absatz 3:

Absatz 3 n. F. enthält die Regelungen des Absatzes 9 a. F.

Zu Absatz 4:

In den Absatz 4 n. F. ist die Regelung des bisherigen § 41 d über die Anwendbarkeit der Bestimmungen des Beschlusses 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6. August 2008, S. 1) bei der polizeilichen Zusammenarbeit mit den Mitgliedstaaten der Europäischen Union überführt worden. Dieser gilt nach Artikel 60 der Richtlinie (EU) 6016/680 weiter fort.

Zu § 41 c

Die Bestimmung des § 41 c n. F. regelt allgemein die Datenübermittlung an Drittstaaten oder internationale zwischen- oder überstaatliche Stellen. Zusätzlich zu § 41 c n. F. ist wie in § 31 n. F. bestimmt, die Regelungen über die Datenübermittlung im Dritten Abschnitt des novellierten Thüringer Datenschutzgesetzes anzuwenden. § 41 c a. F. wird wegen der Neustrukturierung der Datenübermittlungsregelungen im innerstaatlichen Bereich, unter den Mitgliedstaaten der Europäischen Union und im internationalen Bereich aufgehoben.

Zu § 41 d

Die Bestimmung des § 41 d n. F. regelt die Fälle, in denen eine Übermittlung von personenbezogenen Daten untersagt wird.

Zu Absatz 1:

Die Übermittlungsverbote nach Absatz 1 gelten für Übermittlungen innerhalb Deutschlands, an Stellen in Mitgliedstaaten der Europäischen Union und an internationale Stellen im Ausland.

Zu Absatz 2:

Die weiteren Übermittlungsverbote nach Absatz 2 gelten nur für Übermittlungen in den Fällen des § 41 b n. F. (Übermittlungen an Mitgliedstaaten der Europäischen Union) und § 41 c n. F. (Übermittlungen im internationalen Bereich).

Die Regelung des § 41 d a. F. über die Anwendbarkeit der Bestimmungen des Beschlusses 2008/615 JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. L 210 vom 6.8.2008, S. 1) ist aus systematischen Gründen in § 41 b Abs. 4 n. F. überführt worden.

Zu Nummer 11 (§ 42)

§ 42 bleibt als Ermächtigungsgrundlage für die Einrichtung eines automatisierten Abrufverfahrens bestehen. Die Unterrichtung des Landesbeauftragten für den Datenschutz in Absatz 2 Satz 2 a. F. wird gestrichen. Eine Unterrichtung des Landesbeauftragten für den Datenschutz ergibt sich nunmehr aus den Bestimmungen des § 53 des novellierten Thüringer Datenschutzgesetzes.

Zu Nummer 12 (§ 43)

Absatz 1 Satz 2 wird in Umsetzung von Artikel 4 Abs. 2 der Richtlinie (EU) 2016/680 dahin gehend geändert, dass ein Abgleich personenbezogener Daten mit dem Inhalt polizeilicher Daten von sonstigen, in Satz 1 nicht genannten Personen, dann zulässig ist, wenn dieser Datenabgleich zur Erfüllung polizeilicher Aufgaben erforderlich ist. Die Erforderlichkeit gilt auch für den Abgleich personenbezogener Daten mit dem Fahndungsbestand.

Zu Nummer 13 (§§ 45 bis 47)

Zu § 45

Die Regelungen des § 45 a. F. werden aufgehoben, weil mit der Regelung in § 35 ThürDSG n. F. eine vergleichbare Regelung geschaffen worden ist.

Zu § 46

Die bisherige Regelung des § 46 zur Errichtungsanordnung wird aufgehoben. Die Richtlinie (EU) 2016/680 sieht das Instrument der Errichtungsanordnung nicht mehr vor.

Zu § 47

§ 47 a. F. wird aufgehoben. Das Auskunftsrecht der betroffenen Person ergibt sich aus dem Verweis in § 31 Abs. 1 n. F. auf die Bestimmungen im Ersten und Dritten Abschnitt des novellierten Thüringer Datenschutzgesetzes.

Zu Nummer 14 (§ 54 Abs. 4)

Es handelt sich um eine redaktionelle Anpassung.

Zu Nummer 15 (Inhaltsverzeichnis)

Es handelt sich um eine redaktionelle Folgeänderung.

**Zu Artikel 5
Änderung des Thüringer Kommunalwahlgesetzes****Zu Nummer 1 (§ 5)****Zu Buchstabe a) aa)**

Der Begriff "Verarbeitung" umfasst nach Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) auch das Erheben und Nutzen von Daten, ohne den Begriffen unterschiedliche Rechtsfolgen zuzuweisen.

Zu Buchstabe a) bb)

Die Änderungen stellen sicher, dass die Daten ohne Einwilligung des Wahlberechtigten nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Da die Daten nicht bei der betroffenen Person erhoben werden, besteht eine Informations- und Hinweispflicht nach der Verordnung (EU) 2016/679. Mit der Einwilligung des Wahlberechtigten dürfen die personenbezogenen Daten auch für zukünftige Wahlen verarbeitet werden. Für die Erteilung der Einwilligung und deren Widerruf gilt die unmittelbar geltende Verordnung (EU) 2016/679.

Zu Buchstabe a) cc)

Siehe Begründung zu a) aa).

Zu Buchstabe b)

Die Übermittlung von Personaldaten zur Sicherstellung der Besetzung von Wahlvorständen unterfällt nicht den in Artikel 23 der Verordnung (EU) 2016/679 genannten Maßnahmen und erlaubt deshalb keine Verarbeitung der zum Zweck der Personalverwaltung erhobenen Daten zu diesem abweichenden Zweck. Die grundsätzlich vorhandene, inhaltlich durch Artikel 21 Abs. 1 der Verordnung (EU) 2016/679 beschränkte Öffnungsklausel führt hier deshalb nicht zur Zulässigkeit einer abweichenden Regelung. Die Verarbeitung bedarf deshalb der Einwilligung der betroffenen Person.

Zu Nummer 2 (§ 36)

Die Änderung trägt dem Grundsatz der Öffentlichkeit und der Transparenz des Wahlgeschehens Rechnung. Transparenz erfordert, dass der gesamte Wahlvorgang und die daraus resultierende Berechnung einer Sitzverteilung vollständig nachvollziehbar und das Wahlergebnis verifizierbar sind. Rechtsstaatlich begründete Öffentlichkeit dient der Transparenz und Kontrollierbarkeit staatlicher Machtausübung. Dies setzt voraus, dass die Handlungen der staatlichen Organe von den Bürgern zur Kenntnis genommen werden können. Dies gilt auch hinsichtlich der Tätigkeit der Wahlorgane. Die Weiterleitung der Inhalte der Wahlvorschläge und des Wahlergebnisses zur statistischen Bearbeitung und zur Information der Öffentlichkeit erfolgt im Zusammenhang mit dem Wahlverfahren und dient der gebotenen Transparenz.

Zu Nummer 3 (§ 41 a)

Die Übergangsbestimmung dient der Rechtssicherheit der bereits festgesetzten Wahlen.

Zu Nummer 4 (Inhaltsverzeichnis)

Es handelt sich um eine redaktionelle Folgeänderung.

Zu Artikel 6**Änderung des Thüringer Beamtengesetzes****Zu Nummer 1 (§ 72 Abs. 7)**

Es handelt sich um eine redaktionelle Anpassung an die Verordnung (EU) 2016/679. Auftragsdatenverarbeitung ist im Rahmen der Artikel 28 und 29 der Verordnung (EU) 2016/679 zulässig.

Zu Nummer 2 (§ 79)

- a) Es erfolgt eine redaktionelle Anpassung, da es keinen Unterschied zwischen dem Begriffspaar "der Personalplanung und des Personaleinsatzes" und dem Begriffspaar "der Personalverwaltung und Personalwirtschaft" gibt. Eine materielle Rechtsänderung ist mit der Änderung nicht verbunden.
- b) Es handelt sich um eine redaktionelle Anpassung an die Begriffsbestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) (Verordnung (EU) 2016/679). In der Verordnung (EU) 2016/679 ist Verarbeiten jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang. Damit wird das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung abgebildet. Die zusätzliche Erlaubnis des Nutzens von Daten ist damit überflüssig. Eine Verarbeitung zu anderen Zwecken liegt nicht vor, wenn Personalaktendaten ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Gleiches gilt im Rahmen der Datensicherung. Mit der Einfügung des Satzes 2 wird auf die Zulässigkeit einer Verarbeitung zu anderen Zwecken in Artikel 6 Abs. 4 der DS-GVO hingewiesen. Eine Verarbeitung zu anderen Zwecken liegt nicht vor, wenn Personalaktendaten ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Gleiches gilt, soweit im Rahmen der Datensicherung oder der Sicherung des ordnungsgemäßen Betriebes eines Datensystems eine nach dem Stand der Technik nicht oder nur mit unverhältnismäßigem Aufwand zu vermeidende Kenntnisnahme von Personalaktendaten erfolgt.
- c) Es handelt sich um eine redaktionelle Anpassung an die Begriffsbestimmungen der Verordnung (EU) 2016/679.
- d) Es handelt sich um eine redaktionelle Anpassung an die Begriffsbestimmungen der Verordnung (EU) 2016/679.

Zu Nummer 3 (§ 80)

- a) Es handelt sich hierbei um eine Klarstellung, dass auch die Verarbeitung von Personalaktendaten im Rahmen einer Auftragsdatenverarbeitung erfolgen kann. Weiterer Regelungen bedarf es dabei nicht, da die Auftragsdatenverarbeitung in den Artikeln 28 und 29 der Verordnung (EU) 2016/679 abschließend geregelt ist. Eine Auftragsdatenverarbeitung ist unter anderem zulässig, soweit sie erforderlich ist, für die Bewilligung, Festsetzung oder Zahlbarmachung von Geldleistungen, für die automatisierte Erledigung von Aufgaben oder zur Durchführung bestimmter ärztlicher Untersuchungen, die für die Erfüllung der Aufgaben des ärztlichen Dienstes erforderlich sind. Der Verantwortliche soll die Einhaltung der beamten- und datenschutzrechtlichen Bestimmungen durch den Auftragsverarbeiter regelmäßig kontrollieren.
- b) Es handelt sich um eine redaktionelle Anpassung.

Zu Nummer 4 (§ 81)

- a) Es handelt sich um die Anpassung an den umfassenden Begriff "Verarbeitung" in Artikel 4 Nr. 2 der Verordnung (EU) 2016/679. Eine materielle Rechtsänderung ist mit der Änderung nicht verbunden.
- b) Es handelt sich um die Anpassung an den umfassenden Begriff "Verarbeitung" in Artikel 4 Nr. 2 der Verordnung (EU) 2016/679. Eine materielle Rechtsänderung ist mit der Änderung nicht verbunden.

Zu Nummer 5 (§§ 83 und 84)

Zu § 83

Die bisherige Anhörung wird zu einer Informationspflicht (Artikel 16 der Verordnung (EU) 2016/679) an den betroffenen Beamten. In dieser Ausgestaltung liegt kein weiteres Betroffenenrecht im Sinne der Verordnung (EU) 2016/679 vor. Die Daten werden nicht bei den Betroffenen erhoben. Stattdessen erhält der Dienstherr die Daten von Dritten. Dies löst die Informationspflicht nach Artikel 14 der Verordnung (EU) 2016/679.

Zu § 84

Zu Absatz 1:

Es handelt sich um eine Anpassung an die Begrifflichkeiten der Verordnung (EU) 2016/679, da die Auskunft nach Artikel 15 der Verordnung (EU) 2016/679 der Oberbegriff ist und grundsätzlich in Form der Anfertigung einer Kopie erfolgt. Diese bestimmen nur, welche Betroffenenrechte es gibt, nicht jedoch wie sie im Einzelfall umzusetzen sind. Diese Änderungen konkretisieren das Verfahren der Auskunftserteilung. Das Recht auf eine Kopie kann nicht eingeschränkt werden, so dass die Bereitstellung von Auszügen, Abschriften, Ablichtungen oder Ausdrucken nicht mehr im Ermessen der Personalreferate liegt und ebenfalls kostenfrei erfolgen muss. Sie kann nur abgelehnt werden, soweit wichtige dienstliche Gründe dem entgegenstehen.

Zu Absatz 2:

Es handelt sich um eine redaktionelle Änderung.

Zu Absatz 3:

Es handelt sich um die Anpassung an den umfänglichen Begriff der Verarbeitung, die das Nutzen mit einschließt. Eine materielle Rechtsänderung ist mit der Änderung nicht verbunden.

Zu Nummer 6 (§ 85)

a) und b)

Es handelt sich um Anpassungen an den umfassenden Begriff "Verarbeitung" in Artikel 4 Nr. 2 Verordnung (EU) 2016/679. Eine materielle Rechtsänderung ist mit der Änderung nicht verbunden.

c) Die Regelung dient zur Klarstellung. Die Bestimmung stellt klar, dass eine Übermittlung von Personalaktendaten für den Fall, dass einzelne Aufgaben der personalverwaltenden einer anderen Stelle übertragen werden, möglich ist.

d) Es handelt sich um eine redaktionelle Anpassung.

e) Es handelt sich um eine redaktionelle Anpassung an die Verordnung (EU) 2016/679.

Zu Nummer 7 (§ 86)

Es handelt sich um eine redaktionelle Anpassung an die bereits bestehenden Fristen im Thüringer Disziplinalgesetz.

Zu Nummer 8 (§ 87)

Es handelt sich um die Anpassung an den umfassenden Begriff "Verarbeitung" in Artikel 4 Nr. 2 der Verordnung (EU) 2016/679. Eine materielle Rechtsänderung ist mit der Änderung nicht verbunden.

Zu Nummer 9

Es handelt sich um eine redaktionelle Anpassung.

Zu Artikel 7

Änderung des Thüringer Personalvertretungsgesetzes

Die Änderung des Verweises ist erforderlich aufgrund der im Hinblick auf die Umsetzung der europarechtlichen Vorgaben der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) und der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) erfolgten Neufassung des Thüringer Datenschutzgesetzes.

Der bisherige § 37 ThürDSG beschreibt Inhalt und Umfang der Kontrollen bei allen öffentlichen Stellen hinsichtlich der Einhaltung datenschutzrechtlicher Bestimmungen durch den Thüringer Landesbeauftragten für den Datenschutz. Diese Kontrollen werden auch künftig von diesem im Rahmen des europarechtlich vorgesehenen Umfangs wahrgenommen.

Um die Rechte der Personalvertretungen im Bereich des Datenschutzes beizubehalten, sollen auch künftig die Ergebnisse dieser Kontrollen durch den Thüringer Landesbeauftragten für den Datenschutz den Personalvertretungen in Kopie zur Verfügung gestellt werden, soweit sie deren Zuständigkeitsbereich betreffen.

Zu Artikel 8 Änderung des Thüringer Informationsfreiheitsgesetzes

Zu Nummer 1 (§ 6 Abs. 2)

Es handelt sich um eine redaktionelle Änderung aufgrund der Neubekanntmachung des Thüringer Verwaltungsverfahrensgesetzes vom 1. Dezember 2014 (GVBl. S. 685).

Zu Nummer 2 (§ 7 Abs. 4)

Es handelt sich um eine redaktionelle Änderung infolge der Normierung im neuen Absatz 7 in § 12.

Zu Nummer 3 (§ 9 Abs. 1)

Es handelt sich um eine Anpassung an die nunmehr durch die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) definierten besonders geschützten personenbezogenen Daten. Artikel 9 Abs. 1 der Verordnung (EU) 2016/679 erweitert die bisher schon nach § 4 Abs. 5 des ThürDSG in der Fassung vom 13. Januar 2012 (GVBl. S. 27), zuletzt geändert durch Artikel 7 des Gesetzes vom 8. August 2014 (GVBl. S. 539), erfassten Daten (aus denen sich die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen ergeben oder aus denen die Gewerkschaftszugehörigkeit hervorgeht sowie von Daten über die Gesundheit oder das Sexualleben) zusätzlich um genetische Daten, biometrische Daten zur eindeutigen Identifizierung und Daten zur sexuellen Orientierung.

Zu Nummer 4 (§ 12)

- a) Da sich mit Inkrafttreten der Verordnung (EU) 2016/679 die Rechtsstellung des Landesbeauftragten für den Datenschutz ändert, kann die Rechtsstellung des Landesbeauftragten für die Informationsfreiheit nicht mehr durch Verweis auf datenschutzrechtliche Bestimmungen geregelt werden. Daher wird in Absatz 2 die Rechtsstellung des Landesbeauftragten für die Informationsfreiheit durch Übernahme der bisher in Bezug genommenen Bestimmungen geregelt. Lediglich der Aufbau und die Sprache der Bestimmungen werden an einigen Stellen angepasst. Inhaltlich ergeben sich damit keine Änderungen zur bestehenden Rechtslage.
- b) Die Aufgabe des Landesbeauftragten für die Informationsfreiheit, über die Einhaltung der Bestimmungen dieses Gesetzes bei den öffentlichen Stellen im Sinne des § 2 Abs. 1 zu wachen, war bisher in Absatz 2 geregelt. Die Bestimmung wird sprachlich angepasst inhaltsgleich in Absatz 4 Satz 2 übernommen, der weitere Aufgaben des Landesbeauftragten für die Informationsfreiheit normiert.

c) Im neuen Absatz 7 wird zum einen die bisher in Absatz 2 enthaltene Bestimmung übernommen, wonach die Aufgabe des Landesbeauftragten für die Informationsfreiheit von dem Landesbeauftragten für den Datenschutz wahrgenommen wird. Zum anderen wird die bisher in § 7 Abs. 4 enthaltene Bestimmung übernommen, wonach sich der Landesbeauftragte für den Datenschutz auf seine institutionelle Garantie nach Artikel 69 der Verfassung des Freistaats Thüringen berufen kann. Die Bestimmung wird zugleich um die in Artikel 52 der Verordnung (EU) 2016/679 normierte Unabhängigkeit des Landesbeauftragten für den Datenschutz erweitert.

Zu Artikel 9 Änderung des Thüringer Stiftungsgesetzes

§ 6 des Thüringer Stiftungsgesetzes vom 16. Dezember 2008 (GVBl. S. 561), zuletzt geändert durch Artikel 2 des Gesetzes vom 13. März 2014 (GVBl. S. 92, 94), regelt Umfang und Inhalt der öffentlichen Bekanntmachung einer anerkannten Stiftung. Öffentlichkeit und Rechtsverkehr sollen über die neu entstandene juristische Person unterrichtet werden. Hierfür ist die Nennung des Stifters nicht erforderlich, sie fällt auch unter keines der von Artikel 6 Abs. 1 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) genannten Kriterien und ist für den allgemeinen Rechtsverkehr ohne Interesse. Schon bisher hat das Thüringer Stiftungsgesetz deshalb dem Stifter das Recht eingeräumt, die Veröffentlichung seines Namens durch einen entsprechenden Antrag abzuwenden. Die Änderung kehrt das bisherige Regel-Ausnahme-Verhältnis um und verlangt vor dem Hintergrund von Artikel 6 Abs. 1 Buchst. a der Verordnung (EU) 2016/679 nunmehr die ausdrückliche Einwilligung des Stifters zu der Veröffentlichung seines Namens.

Zu Artikel 10 Änderung des Thüringer Rettungsdienstgesetzes

Durch Artikel 10 werden die speziellen Datenschutzregelungen in § 30 Thüringer Rettungsdienstgesetz formalrechtlich an die Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) angepasst. Eine inhaltliche Änderung der verordnungskonformen Datenschutzregelungen ist damit nicht verbunden.

Zu Nummer 1

Aufgrund des Inkrafttretens der Verordnung (EU) 2016/679 und der damit verbundenen unmittelbaren Geltung ab dem 25. Mai 2018 wird das Datenschutzrecht durch unmittelbar geltende Bestimmungen der Verordnung und ergänzend des neugefassten Thüringer Datenschutzgesetzes geprägt.

Zu Nummer 2

Über den Verarbeitungsbegriff in Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 wird künftig als Unterfall unter anderem auch das Nutzen be-

ziehungsweise Verwenden erfasst. Somit ist die bisherige alternative Nennung des Begriffs "Nutzen" obsolet.

Zu Nummer 3

Mit der Änderung wird der bisherige Begriff "Nutzen" an den in Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 gebrauchten Begriff "Verwenden" terminologisch angepasst.

Zu Nummer 4

Es handelt sich um eine redaktionelle Anpassung an den Wortlaut von Artikel 23 Abs. 1 Buchst. i) der Verordnung (EU) 2016/679. In Verbindung mit Artikel 6 Abs. 4 der Verordnung (EU) 2016/679 gibt die Bestimmung vor, unter welchen Voraussetzungen Daten zu anderen Zwecken verarbeitet und damit übermittelt werden dürfen.

Zu Nummer 5

Zu Buchstaben a) und b)

Mit den Änderungen wird der bisherige Begriff "Nutzen" an den in Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 gebrauchten Begriff "Verwenden" terminologisch angepasst.

Zu Buchstabe c)

Über den Verarbeitungsbegriff in Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 wird künftig als Unterfall unter anderem auch das Nutzen beziehungsweise Verwenden erfasst. Somit ist die bisherige alternative Nennung des Begriffs "Nutzen" obsolet.

Zu Artikel 11

Änderung des Thüringer Vermessungs- und Geoinformationsgesetzes

Mit der Regelung werden aufgrund Artikel 23 Abs. 1 Buchst. e) der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) die Informationspflicht nach Artikel 13 und 14, das Recht auf Berichtigung nach Artikel 16, das Recht auf Einschränkung der Verarbeitung nach Artikel 18 und das Widerspruchsrecht nach Artikel 21 der Verordnung (EU) 2016/679 eingeschränkt. Die Einschränkung ist vertretbar, da im Liegenschaftskataster die Eigentümerangaben lediglich nachrichtlich in Übereinstimmung mit dem Grundbuch geführt werden. Bezüglich der ergänzenden Angaben ist die beschriebene Einschränkung auch vertretbar, da die Informationspflicht zu einem unzumutbaren hohen Aufwand der Verwaltung führen würde. Die Betroffenenrechte bleiben aber weiterhin erhalten, da sie vorbehaltlich abweichender bereichsspezifischer Regelungen bei dem für die Führung der Eigentumsangaben originär zuständigen Grundbuchamt geltend gemacht werden können. Die Einschränkung der Betroffenenrechte sollte aber dann nicht gelten, wenn die betroffene Person geltend macht, dass die im Liegenschaftskataster nachrichtlich geführten Eigentumsangaben nicht mit der Originalquelle, dem Grundbuch, übereinstimmen. Damit wird die bisherige abweichende Regelung

zum Thüringer Datenschutzgesetz weiter beibehalten und lediglich entsprechend angepasst.

Zu Artikel 12

Änderung des Thüringer Hochschulgebühren- und -entgeltgesetzes

Die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) verlangt stets eine Rechtsgrundlage für die Zulässigkeit der Datenverarbeitung, diese soll hiermit ausdrücklich in das Thüringer Hochschulgebühren- und -entgeltgesetz eingefügt werden.

Zu Artikel 13

Änderung des Thüringer Schulgesetzes

Zu Nummer 1 (§ 57)

Die Begrifflichkeiten des § 57 ThürSchulG werden an die Begrifflichkeiten der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) angepasst.

Nach Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 umfasst die "Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. In § 57 ThürSchulG wird daher ausschließlich der Begriff "verarbeiten" verwendet. Der Begriff "Betroffener" wird durch die "betroffene Person" ersetzt (vergleiche Artikel 4 Nr. 1 der Verordnung (EU) 2016/679).

Die zulässige Datenverarbeitung nach Absatz 1 umfasst auch die Berechtigung der öffentlichen Stelle, personenbezogene Daten der Schüler, Eltern, Lehrer, Erzieher und Sonderpädagogischen Fachkräfte zu erheben. Daraus lässt sich spiegelbildlich eine Verpflichtung der betroffenen Personen ableiten, dem Verantwortlichen die erforderlichen personenbezogenen Daten auch zur Verfügung zu stellen. Absatz 2 Satz 1 bleibt als deklaratorischer Satz erhalten. Satz 2 kann jedoch entfallen, da abschließende und umfassende Regelungen zu den Informationspflichten des Verantwortlichen bei Erhebung von personenbezogenen Daten gegenüber der betroffenen Person sowohl Artikel 13 der Verordnung (EU) 2016/679 sowie § 20 Thüringer Datenschutzgesetz (ThürDSG) enthalten.

Die Verordnung (EU) 2016/679 sieht für mitgliedstaatliche bereichsspezifische Rechtsgrundlagen der Verarbeitung Öffnungsklauseln in Artikel 6 Abs. 1 lit. c und e vor. Für die Rechtsgrundlagen der Verarbeitung, die nach Artikel 6 Abs. 1 lit. a, b, d und f der Verordnung (EU) 2016/679 unmittelbar gelten, besteht kein nationaler Regelungsspielraum. Daher dürfen insbesondere keine nationalen bereichsspezifischen Regelungen zur Einwilligung getroffen werden, die eine Einschränkung der Verarbei-

tung durch Formerfordernisse, wie etwa einer "schriftlichen" Einwilligung vorsehen. Absatz 3 Satz 2 wird insoweit angepasst. Die Voraussetzungen für eine wirksame Einwilligung sind in Artikel 7 der Verordnung (EU) 2016/679 normiert. Entscheidend ist dabei die Nachweispflicht des Verantwortlichen über die erteilte Einwilligung.

Der Begriff der Verarbeitung schließt auch die Datenübermittlung mit ein. Wann eine Verarbeitung personenbezogener Daten rechtmäßig ist, legen Artikel 6 der Verordnung (EU) 2016/679 sowie §§ 16, 17 ThürDSG fest. Eine gesonderte Regelung einzelner Tatbestände der Datenübermittlung, wie sie der aufzuhebende Absatz 4 vorsieht, ist nicht erforderlich. Die Übermittlung personenbezogener Daten an die Gesundheitsämter ist erforderlich, um die ihnen nach § 55 ThürSchulG übertragene Aufgabe der Schulgesundheitspflege, die auch die Durchführung schulärztlicher Untersuchungen umfasst, wahrzunehmen. Die Aufgaben der Jugendämter im Rahmen des Kinderschutzes regeln insbesondere § 55 a ThürSchulG, das Sozialgesetzbuch VIII sowie das Gesetz zur Kooperation und Information im Kinderschutz.

Die Verarbeitung umfasst nach Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 auch die "Verbreitung oder eine andere Form der Bereitstellung" personenbezogener Daten, mithin auch die Veröffentlichung in Jubiläums- und Jahresberichten oder Klassenübersichten. Hier werden personenbezogene Daten veröffentlicht, die gerade nicht für diesen Zweck, sondern zum Beispiel bei der Aufnahme in die Schule nach § 136 Abs. 1 Thüringer Schulordnung erhoben wurden. § 17 Abs. 2 ThürDSG regelt unter Berufung auf Artikel 6 Abs. 4 der Verordnung (EU) 2016/679 die Weiterverarbeitung zu anderen Zwecken als denen, zu denen die Daten erhoben wurden. Die Weiterverarbeitung zu anderen Zwecken ist nur zulässig, wenn die betroffene Person eingewilligt hat oder die Weiterverarbeitung auf eine Rechtsgrundlage gestützt werden kann, die eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Abs. 1 der Verordnung (EU) 2016/679 genannten Ziele darstellt. § 17 Abs. 2 ThürDSG schafft hierfür landesrechtliche Rechtsgrundlagen und öffnet so die Möglichkeit eines Datenumgangs aus anderen als den ursprünglichen Erhebungszwecken. Die Veröffentlichung in Jubiläums- und Jahresberichten oder Klassenübersichten wird vom Katalog des § 17 Abs. 2 ThürDSG nicht umfasst. Daher bedarf es in den Fällen des aufzuhebenden Absatzes 7 einer Einwilligung der betroffenen Person nach Maßgabe des Artikels 7 der Verordnung (EU) 2016/679; ein bloßes Widerspruchsrecht ist nicht ausreichend. Da die Veröffentlichung in Jubiläums- und Jahresberichten oder Klassenübersichten folglich nur im Rahmen der allgemeinen Bestimmungen des Thüringer Datenschutzgesetzes und der Verordnung (EU) 2016/679 erfolgen kann, ist Absatz 7 ersatzlos aufzuheben.

Die Ermächtigungsgrundlage in Absatz 8 Nummer 3 führt allein von ihrem Wortlaut her dazu, dass jeder Verwendungszweck beim Einsatz automatisierter Verfahren ausdrücklich in einer Rechtsverordnung geregelt werden müsste. Der Begriff des Verarbeitens nach Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 umfasst von seiner Definition her auch jeden mit Hilfe automatisierter Verfahren ausgeführten Vorgang. Soweit die Verarbeitung nach den geltenden Rechtsgrundlagen zulässig ist, kann diese folglich immer auch mit Hilfe automatisierter Verfahren erfolgen, ohne dass es hierfür einer gesonderten Regelung bedarf.

Die Verordnungsermächtigung kann daher auf den in § 136 Abs. 10 Thüringer Schulordnung speziell geregelten Einsatz von automatisierten Abrufverfahren in Krisen- oder Notfällen beschränkt werden.

Zu Nummer 2 (§ 58)

Die Begrifflichkeiten des § 58 ThürSchulG werden an die Begrifflichkeiten der Verordnung (EU) 2016/679 angepasst.

Nach Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 umfasst die "Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. In § 58 ThürSchulG wird daher ausschließlich der Begriff "verarbeiten" verwendet.

Zu Nummer 3 (§ 60)

Die Begrifflichkeiten des § 60 ThürSchulG werden an die Begrifflichkeiten der Verordnung (EU) 2016/679 angepasst; es handelt sich insoweit um eine Folgeänderung zu den Änderungen nach den Nummern 1 und 2.

Zu Artikel 14**Änderung des Thüringer Gesetzes zur Ausführung des Artikel 10-Gesetzes**

Es handelt sich um eine Folgeänderung der neuen Begriffsdefinitionen in § 32 Thüringer Datenschutzgesetz (ThürDSG) zum Umgang mit personenbezogenen Daten.

Zu Artikel 15**Änderung des Thüringer Verfassungsschutzgesetzes****Zu Nummer 1 Buchstabe a (§ 2 Abs. 5 Satz 2)**

Es handelt sich um eine redaktionelle Anpassung an die im Übrigen im Gesetz verwendeten Begrifflichkeiten.

Zu Nummer 1 Buchstabe b (§ 2 Abs. 5 Satz 3)

Es handelt sich um eine redaktionelle Anpassung an die auch im Übrigen verwendeten Begrifflichkeiten für Regelungen zur Ausgestaltung innerbehördlicher Arbeitsabläufe.

Zu Nummer 2 (§ 6 Abs. 2)

Es handelt sich um eine Anpassung entsprechend der auch für das Amt für Verfassungsschutz verbindlichen bundesgesetzlichen Regelung in § 3 Abs. 1 in Verbindung mit § 4 Abs. 2 BVerfSchG. Im Sinne einer klaren Vorgabe wird deutlich gemacht, dass maßgeblicher Bezugspunkt für die Auslösung eines gesetzlichen Beobachtungsauftrages und einer damit korrespondierenden Verpflichtung im Rahmen von § 4 Abs. 1 in Verbindung mit § 6 Abs. 1 Nr. 3 ThürVerfSchG die Gefährdung solcher elementarer Wertentscheidungen der verfassungsmäßigen Ordnung in Bund und Ländern ist, wie sie durch das Bundesverfassungsgericht herausgearbeitet wurden. Eine Fortentwicklung und Bestimmung dessen, was Merkmal der freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes ist, bleibt diesem vorbehalten. Demgegenüber erreichen Bestrebungen, die sich gegen ein Recht auf Bildung und gegen

Maßnahmen der Wirtschafts- und Arbeitsförderung sowie der Daseinsvorsorge richten, wesensmäßig nicht eine vergleichbare Bedeutung, die geeignet wäre, einen gesetzlichen Beobachtungsauftrag auszulösen.

Zu Nummer 3 (§ 7 Abs. 1)

§ 7 Abs. 1 Satz 1 wird redaktionell den neuen Begrifflichkeiten des Thüringer Datenschutzgesetzes angepasst und entsprechend dem Regelungsvorbild des Bundesgesetzgebers um einen Halbsatz ergänzt, der die Verarbeitung auch nach Einwilligung regelt. Damit wird einem fundamentalen Grundsatz des Datenschutzrechts Rechnung getragen, wie er bislang in § 4 Abs. 1 ThürDSG a. F. niedergelegt war und im Übrigen auch bereits an anderer Stelle im Gesetz (§ 30 Abs. 3 Satz 1) wiedergegeben ist. Die Einzelheiten der Einwilligung sind in § 39 Abs. 1 bis 4 ThürDSG geregelt, der über § 36 entsprechende Anwendung findet. Praktisch bedeutsam wird die Einwilligung vor allem in Akkreditierungsfällen, wenn beispielsweise ein Dateiabgleich zum Einwilligenden für eine Risikoüberprüfung vor Zutrittsgewährung in einen besonders geschützten Bereich stattfinden soll.

Zu Nummer 4 Buchstabe a (§ 8 Abs. 2)

Die Änderung dient der Behebung eines redaktionellen Fehlers in der verkündeten Gesetzesfassung (GVBl. S. 529 ff). Dem bisherigen § 8 Abs. 2 Satz 3 fehlt im Wortlaut der Norm der Gegenstand der durch Rechtsverordnung zu regelnden Einzelheiten der Auskunftserteilung. Dem wird im Interesse der Rechtsharmonisierung durch Verweis auf die bundesrechtlichen Vorgaben in der jeweils geltenden Fassung abgeholfen (§ 8b Abs. 10 Satz 3 BVerfSchG).

Zu Nummer 4 Buchstabe b (§ 8 Abs. 2 a)

Es handelt sich um eine Folgeänderung zur Änderung von § 93 Abs. 8 Abgabenordnung durch das Gesetz zur Umsetzung der Vierten EU-Geldwäscherichtlinie, zur Ausführung der EU-Geldtransferverordnung und zur Neuorganisation der Zentralstelle für Finanztransaktionsuntersuchungen (BGBl. I, S. 1822 ff). Durch Verweis auf die bundesgesetzliche Regelung in der jeweils geltenden Fassung wird ein Anwendungsdefizit bei der Einholung von Auskünften nach Absatz 2 Satz 1 Nr. 2 beseitigt. Praktische Relevanz kann die Regelung im Vorfeld von Auskünften nach § 8 Abs. 2 Satz 1 Nr. 2 insbesondere bei der Aufklärung von Finanzierungsströmen und -mitteln von großangelegten Szeneveranstaltungen (zum Beispiel sogenannte Rechtsrockkonzerte), unternehmerischen Beziehungsgeflechten (zum Beispiel Vertrieb von Szenedevotionalien durch Extremisten) oder Immobilienerwerben erlangen, die für Beteiligte erhebliche finanzielle Anreize liefern und von besonderer Relevanz für die Etablierung und Festigung des Zusammenhalts innerhalb aufzuklärender extremistischer Gruppierungen sind.

Zu Nummer 4 Buchstabe c (§ 8 Abs. 4)

Es handelt sich um Folgeänderungen der neuen Begriffsdefinitionen in § 32 ThürDSG zum Umgang mit personenbezogenen Daten.

Zu Nummer 5 (§ 13 Abs. 3)

Die Änderungen zu den Buchstaben a) und b) sind Folgeänderungen der neuen Begriffsdefinitionen in § 32 des ThürDSG und stellen in Buchstabe c) die Beschränkungen bei der Verarbeitung in elektronischen Akten klar.

Zu Nummer 6 (§ 16 Abs. 1)

Es handelt sich um eine Folgeänderung der neuen Begriffsdefinitionen in § 32 ThürDSG zum Umgang mit personenbezogenen Daten.

Zu Nummer 7 (§ 18 Abs. 1)

Es handelt sich um eine zur Vermeidung von Doppelbefassungen vorgenommene klare Zuständigkeitskonzentration bei der G10-Kommission des Thüringer Landtages. Diese übt als parlamentarisches Fachgremium nach § 11 Abs. 4 Satz 5 in Verbindung mit § 8 Abs. 4 und 5 die Kontrolle über die gesamte Verarbeitung der durch den Einsatz erhobenen Daten aus. Die Unterrichtungspflicht der Landesregierung nach § 11 Abs. 4 Satz 5 in Verbindung mit § 8 Abs. 6 sowie § 27 gegenüber der Parlamentarischen Kontrollkommission im Übrigen bleiben hiervon unberührt. Auch die Prüfung einer Benachrichtigung der betroffenen Person ist bereits aufgrund der bestehenden Regelung des § 11 Abs. 4 Satz 5 in Verbindung mit § 8 Abs. 5 Satz 2 sichergestellt.

Zu Nummer 8 (§ 22 Abs. 2)

Es handelt sich um eine redaktionelle Anpassung an eine neue Paragrafenfolge im Bundesverfassungsschutzgesetz. Im Übrigen ist bereits bundesgesetzlich durch § 6 Abs. 1 Satz 2 BVerfSchG bzw. ausgesprochene Weitergabebeschränkungen verbindlich klargestellt und durch die Rechtsprechung anerkannt (vgl. BVerfG, Beschluss vom 13.10.2016 - Az. 2 BvE 2/15, BVerwG, Beschluss vom 29.04.2015 - Az. 20 F 8.14, BVerwG, Beschluss vom 20.07.2015 - Az. 6 VR 1.15, BVerwG, Beschluss vom 07.08.2013 - Az. 20 F 9/12), dass eine Weitergabe von Informationen, die dem Amt für Verfassungsschutz durch andere Nachrichtendienste im Rahmen des Informationsaustausches nach Maßgabe der anwendbaren fachgesetzlichen Regelungen übermittelt worden sind, an dritte Stellen nur mit Zustimmung des Nachrichtengebers erfolgen darf.

Zu Nummer 9 (§ 36)

Es handelt sich um erforderliche Anpassungen infolge der Neufassung des Thüringer Datenschutzgesetzes. Ähnlich der bisherigen Systematik dient die ergänzende Anwendbarkeit aus Gründen der Normenklarheit abschließend aufgeführter einzelner Regelungen des neu gefassten Thüringer Datenschutzgesetzes zugleich der Rechtsharmonisierung. Dies gilt beispielsweise im Hinblick auf die Funktion des Datenschutzbeauftragten nach § 13 ff. ThürDSG, die Anforderungen für technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung sowie die Regelung zu einzelnen relevanten Begrifflichkeiten nach dem hierzu für entsprechend anwendbar erklärten § 32 ThürDSG, die im Interesse einer überwiegend einheitlichen datenschutzrechtlichen Terminologie einbezogen wird. Im Übrigen geben bereits die bereichsspezifischen bundes- und landesgesetzlichen Regelungen ein im Sinne des § 2 Abs. 4 ThürDSG abschließendes nationales Datenschutzvollregime im Zusammenhang mit der Aufgabenerfüllung nach § 4 vor, die dem Anwendungsbereich beider Unionsrechtsakte nicht unterfällt (Artikel 4 Abs. 2 Satz 3 EUV in Verbindung mit Artikel 2 Abs. 2 Buchst. a) Verordnung 2016/679 und Artikel 2 Abs. 3 Buchst. a) Richtlinie 2016/680) und die daher den anwendbaren nationalen Regelungen über den bereichsspezifischen Datenschutz unterworfen bleibt.

**Zu Artikel 16
Änderung des Thüringer Sicherheitsüberprüfungsgesetzes****Zu Nummer 1 (§ 6)**

Es handelt sich um eine redaktionelle Anpassung infolge der Neufassung des Thüringer Datenschutzgesetzes (ThürDSG).

Zu Nummer 2 (§ 22)

Es handelt sich um eine Folgeänderung der neuen Begriffsdefinitionen in § 32 ThürDSG zum Umgang mit personenbezogenen Daten.

Zu Nummer 3 (§ 23)

Es handelt sich um Folgeänderungen der neuen Begriffsdefinitionen in § 32 ThürDSG zum Umgang mit personenbezogenen Daten.

Zu Nummer 4 (§ 24 Abs. 4)

Die redaktionellen Ergänzungen dienen der sprachlichen Vereinheitlichung.

Zu Nummer 5 (§ 36)

Es handelt sich um einen Verweis auf einzelne anzuwendende Regelungen des Thüringer Datenschutzgesetzes. Die Regelung ist für den Bereich des Sicherheitsüberprüfungsrechtes vergleichbar der Anpassung in § 36 ThürVerfSchG n. F., so dass auf die dortigen Ausführungen verwiesen wird.

Zu Nummer 6

Es handelt sich um gesetzessystematische Folgeanpassungen zu den vorgenannten Änderungen.

**Zu Artikel 17
Änderung des Thüringer Statistikgesetzes****Zu Nummer 1 (§ 3)**

Die Verweise auf das Thüringer Datenschutzgesetz sowie die §§ 8, 9 ThürDSG sind anzupassen. § 8 ist nunmehr § 19 ThürDSG, § 9 entspricht Artikel 32 der Verordnung (EU) 2016/679. Die Regelung zur Datenschutzaufsicht findet sich in den §§ 3 bis 12 ThürDSG. Insofern handelt es sich lediglich um redaktionelle Änderungen. Mit Satz 1 wird von der Öffnungsklausel des Artikels 89 der Verordnung (EU) 2016/679 Gebrauch gemacht.

Die Gesamtverantwortung des Verantwortlichen mit sämtlichen Rechten und Pflichten ergibt sich nunmehr aus Artikel 5 Abs. 2 sowie Kapitel IV der Verordnung (EU) 2016/679.

Zu Nummer 2 (§ 18)

Die Datenverarbeitung zur Durchführung von wissenschaftlichen Forschungsvorhaben ist in Artikel 5 Abs. 1 Buchst. b und in Artikel 6 der Verordnung (EU) 2016/679 sowie ergänzend in § 28 ThürDSG geregelt. Zu diesem Zweck dürfen Daten stets weiterverarbeitet werden. Das Anknüpfen an zusätzliche Voraussetzungen ist nicht vorgesehen.

Zu Nummer 3 (§ 19)

- a) Es handelt sich bei § 19 um eine Informationspflicht an betroffene Personen. Diese ist vorrangig in Artikel 13 der Verordnung (EU) 2016/679 geregelt. § 19 hat daher unter datenschutzrechtlichen Aspekten nur noch ergänzenden Charakter. Dies wird im Einleitungssatz klar gestellt.
- b) Um Wiederholungen zu vermeiden, werden in Ziffer 1 diejenigen Informationen gestrichen, über die der Verantwortliche bereits nach Artikel 13 Abs. 1 Buchst. c der Verordnung (EU) 2016/679 zu unterrichten hat.

Zu Artikel 18**Änderung des Thüringer Gesetzes zur Ausführung der Verwaltungsgerichtsordnung**

Mit Inkrafttreten des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU vom 30. Juni 2017 (BGBl. I S. 2097) und des mit dessen Artikel 1 konstitutiv neu gefassten Bundesdatenschutzgesetzes (BDSG) sind spezielle Thüringer Regelungen zum Verfahrensrecht für Verwaltungsakte der Aufsichtsbehörde für den Datenschutz im nichtöffentlichen Bereich nach § 38 Abs. 6 BDSG in der bis zum 24. Mai 2018 geltenden Fassung nicht mehr notwendig. Das Entfallen des Vorverfahrens gegen Verwaltungsakte der Aufsichtsbehörde für Datenschutz sowie die Beteiligtenfähigkeit der nach Landesrecht zuständigen Aufsichtsbehörde, die nach § 40 Abs. 1 BDSG in der ab 25. Mai 2018 geltenden Fassung zu bestimmen ist, sind zukünftig in § 20 BDSG in der ab 25. Mai 2018 geltenden Fassung geregelt.

Zu Artikel 19**Änderung des Thüringer Gesetzes zur Umsetzung der Bestimmungen über die europäische Amtshilfe**

Durch die Änderung wird die Diktion des Thüringer Gesetzes zur Umsetzung der Bestimmungen über die europäische Amtshilfe an die Diktion in Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) angepasst.

Zu Artikel 20**Änderung des Thüringer Tiergesundheitsgesetzes**

Aufgrund der Begriffsbestimmung in Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) handelt es sich bei der Nutzung personenbezogener Daten um eine Verarbeitung. Es wird daher künftig in § 35 Satz 1 allein auf die Verarbeitung der Daten Bezug genommen.

**Zu Artikel 21
Änderung des Thüringer Landesmediengesetzes**

Mit Artikel 21 werden die Regelungen des Thüringer Landesmediengesetzes (ThürLMG) vom 15. Juli 2014 (GVBl. S. 385), geändert durch das Thüringer Gesetz zu dem Siebzehnten Rundfunkänderungsstaatsvertrag vom 23. September 2015 (GVBl. S. 134) geändert.

Bisher regelt § 6 ThürLMG die beschränkte Anwendbarkeit von Datenschutzrecht und Datenschutzaufsicht auf Medien und Presse. Dieses sogenannte Medienprivileg aus Artikel 5 Abs. 1 Grundgesetz ist Ausfluss der Medien- und Pressefreiheit, insbesondere mit Blick auf den journalistischen Quellenschutz und das Schutzgut des Recherchegeheimnisses. Ab dem 25. Mai 2018 gilt die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz der natürlichen Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) und somit das dort verankerte Datenschutzrecht unmittelbar. Die Verordnung (EU) 2016/679 selbst sieht kein Medienprivileg vor, sondern gibt es den Mitgliedstaaten auf, das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken, in Einklang zu bringen (vgl. Artikel 85 Abs. 1 und 2 Verordnung (EU) 2016/679).

Mit der Neufassung des § 6 ThürLMG erfolgt somit diese spezialgesetzliche Möglichkeit der Verankerung des Medienprivilegs durch eine Anwendung lediglich der Kapitel I (Allgemeine Bestimmungen), Kapitel VIII (Rechtsbehelfe, Haftung und Sanktionen), Kapitel X (Delegierte Rechtsakte und Durchführungsrechtsakte) und Kapitel XI (Schlussbestimmungen) sowie der Artikel 5 Abs. 1 Buchst. f (Zweckbindung) in Verbindung mit Abs. 2 (Rechenschaftspflicht), Artikel 24 (Verantwortung des für die Verarbeitung Verantwortlichen) und Artikel 32 (Sicherheit der Verarbeitung) der Verordnung (EU) 2016/679. Durch die in § 1 Abs. 7 ThürLMG geltende dynamische Generalverweisung auf die rundfunkrechtlichen Staatsverträge in ihrer jeweilig geltenden Fassung ist auch die Durchwirkung dieser Regelungen, wie derzeit zum Beispiel der §§ 47 und 57 Rundfunkstaatsvertrag (RfStV) sowie auch geplanter Neuerungen, wie zum Beispiel des vorgesehenen § 9c RfStV-E, stets gewährleistet, bei gleichfalls prominent im Thüringer Landesmediengesetz genannten Medienprivileg.

**Zu Artikel 22
Änderung des Thüringer Pressegesetzes**

Mit Artikel 22 werden die Regelungen des Thüringer Pressegesetzes (TPG) vom 31. Juli 1991 (GVBl. S. 271), zuletzt geändert durch Artikel 3 des Gesetzes vom 16. Juli 2008 (GVBl. S. 243), geändert.

Bisher regelt § 11 a TPG die beschränkte Anwendbarkeit von Datenschutzrecht und Datenschutzaufsicht auf die Presse. Dieses sogenannte Medienprivileg aus Artikel 5 Abs. 1 Grundgesetz ist Ausfluss der Pressefreiheit, insbesondere mit Blick auf den journalistischen Quellenschutz und das Schutzgut des Recherchegeheimnisses. Ab dem 25. Mai 2018 gilt die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz der natürlichen Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) und

somit das dort verankerte Datenschutzrecht unmittelbar. Die Verordnung (EU) 2016/679 selbst sieht kein Medienprivileg vor, sondern gibt es den Mitgliedstaaten auf, das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit, einschließlich der Verarbeitung zu journalistischen Zwecken, in Einklang zu bringen (vergleiche Artikel 85 Abs. 1, 2 Verordnung (EU) 2016/679). Gerade im Pressebereich ist eine journalistische Tätigkeit ohne staatliche Einfluss- und Kontrollmöglichkeiten von besonderer Bedeutung und angesichts der grundlegenden Aufgaben ("Wächteramt" der Presse) ein unverzichtbares und auch grundrechtlich gebotenes Element.

Mit der Neufassung von § 11 a TPG wird dieser Auftrag für die Presse erfüllt. Die Freistellung der Presseunternehmen von den meisten datenschutzrechtlichen Pflichten und deren Überwachung (sogenanntes Medienprivileg) für die journalistisch-redaktionellen und literarischen Zwecken dienende Datenverarbeitung wird in § 11 a des TPG geregelt.

Die in einem freien demokratischen Gemeinwesen grundlegende, keiner staatlichen Kontrolle unterliegende Pressefreiheit wird durch Artikel 11 Abs. 2 der Charta der Grundrechte der Europäischen Union und außerdem durch Artikel 10 der Europäischen Menschenrechtskonvention sowie durch Artikel 5 Abs. 1 des Grundgesetzes besonders geschützt. Auf die besondere Bedeutung des durch Artikel 11 der Grundrechtecharta gewährleisteten Grundrechts der Meinungs- beziehungsweise Pressefreiheit als "eine der wesentlichen Grundlagen einer demokratischen und pluralistischen Gesellschaft", die nur soweit erforderlich eingeschränkt werden dürfe, hat der Gerichtshof der Europäischen Union mehrfach hingewiesen (Urteil der Großen Kammer vom 21.12.2016 Rs. C-203/15 u. a. m. w. N.; zur Pressefreiheit vergleiche Urteil vom 12.9.2007 Rs. T-36/04).

Der Schutzbereich der Pressefreiheit ist grundsätzlich weit und reicht von der Informationsbeschaffung über die Informationsbearbeitung bis hin zur Informationsverbreitung. Die Presse ist bei Erfüllung ihrer verfassungsrechtlich verbürgten Aufgabe bei der öffentlichen und individuellen Meinungsbildung zwingend auf die Verwendung personenbezogener Daten angewiesen. Journalistische Arbeit, vor allem auch eine verdeckte Recherche im Rahmen eines investigativen Journalismus, wäre ohne die Möglichkeit, personenbezogene Daten auch ohne Einwilligung der betroffenen Personen zu erheben, zu speichern und zu nutzen, nicht möglich. Entsprechendes gilt, wenn den betroffenen Personen konkrete Auskunft- und daraus folgende Berichtigungsansprüche zu nicht veröffentlichten redaktionellen Daten eingeräumt würden. Einflüsse von außen auf diese Daten vor allem im Vorfeld der Berichterstattung müssen deshalb weitestmöglich von vornherein vermieden werden. Das Medienprivileg soll verhindern, dass der Datenschutz freier journalistischer Tätigkeit entgegensteht. Geschützt werden hierdurch nicht nur die Journalisten, sondern auch Informanten und sonstige Betroffene. Erfasst wird insbesondere auch der Schutz der Quellen der Journalisten und die Speicherung und sonstige Verarbeitung personenbezogener Daten, etwa in Redaktions- oder Nachrichtenarchiven.

Der Europäische Gerichtshof für Menschenrechte hat in seiner Rechtsprechung mehrfach die grundlegende Bedeutung und das große Gewicht der Pressefreiheit für eine demokratische Gesellschaft, die unentbehrliche Rolle der Presse als "Wachhund" und die staatliche Verpflichtung, die Pressefreiheit zu gewährleisten und zu erhalten, betont und insbesondere auch den Quellenschutz als Eckstein der Pressefrei-

heit bezeichnet, ohne den Informanten davon abgehalten werden könnten, der Presse bei der Unterrichtung der Öffentlichkeit über Fragen öffentlichen Interesses zu helfen (zum Beispiel Urteile vom 28.6.2012, NJW 2013, 3709, vom 19.1.2016, NJW 2017, 1533 und vom 21.1.2016, NJW 2017, 795 je m. w. N.).

Auch das Bundesverfassungsgericht hat in ständiger Rechtsprechung eine freie, nicht von der öffentlichen Gewalt gelenkte, vom Staat unabhängige, keiner Zensur unterworfen freie Presse als Wesenselement des freiheitlichen Staats und als für die moderne Demokratie unentbehrlich angesehen; es hat mehrfach festgestellt, dass auch die Geheimhaltung der Informationsquellen und das Vertrauensverhältnis zwischen Presse und Informanten geschützt und dieser Schutz unentbehrlich ist (BVerfGE 117, 244, 258 f. m. w. N.).

Dementsprechend ist auch das Bundesverwaltungsgericht zu dem die Presse von der Einhaltung von Datenschutzbestimmungen weitgehend freistellenden Medienprivileg davon ausgegangen, dass ohne eine Datenverarbeitung auch ohne Einwilligung der Betroffenen journalistische Arbeit nicht möglich wäre (BVerwG, Beschluss vom 29.10.2015 - 1 B 32/15).

Der Umfang des Medienprivilegs beruht auf einer Abwägung mit den Persönlichkeitsrechten der Betroffenen und dem daraus abgeleiteten Schutz seiner persönlichen Daten. Dieser Schutz wird europarechtlich durch Artikel 8 der EU-Grundrechtecharta sowie durch Artikel 8 der Europäischen Menschenrechtskonvention und grundgesetzlich durch Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 Grundgesetz gewährleistet.

Zu Artikel 23

Änderung des Thüringer Gesetzes über das Verfahren bei Einwohnerantrag, Bürgerbegehren und Bürgerentscheid

Der Gesetzestext wird redaktionell an Artikel 4 Nr. 2 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72) angepasst. Der bisher verwendete Begriff "nutzen" wird von dem in der Verordnung (EU) 2016/679 verbindlich definierten Oberbegriff "verarbeiten" mit umfasst.

Zu Artikel 24

Änderung des Thüringer Berufsqualifikationsfeststellungsgesetzes (ThürBQFG)

Zu Nummer 1 (§ 1)

Es handelt sich um eine redaktionelle Änderung.

Zu Nummer 2 (§ 13 b)

- a) Vor dem Hintergrund der unmittelbaren Geltung der Verordnung (EU) 2016/679 hat der Absatz nur noch deklaratorische Wirkung und kann daher aufgehoben werden.
- b) Es handelt sich um eine redaktionelle Änderung.
- c) Es handelt sich um eine redaktionelle Änderung.
- d) Es handelt sich um eine redaktionelle Änderung.

Zu Nummer 3 (§ 16 Abs. 6)

§ 3 Abs. 1 des Thüringer Datenschutzgesetzes enthielt ein grundsätzliches Verbot der Verarbeitung "besonderer Arten personenbezogener Daten", "aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben hervorgehen". Durch einen Verweis auf diesen Katalog wurde die in § 16 Abs. 6 Nr. 2 des Thüringer Berufsqualifikationsfeststellungsgesetzes vom 16. April 2014 (GVBl. S. 139), zuletzt geändert durch Artikel 1 des Gesetzes zur Änderung des Thüringer Anerkennungsgesetzes und anderer Gesetze vom 2. Juli 2016 (GVBl. S. 229), enthaltene Ermächtigung, durch Rechtsverordnung neue Merkmale für die amtliche Statistik einzuführen, eingeschränkt.

Auch in der unmittelbar geltenden Verordnung (EU) 2016/679 ist mit Artikel 9 Abs. 1 ein solcher Katalog enthalten. Er umfasst das Verbot der "Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person" unter der Bezeichnung "besondere Kategorien personenbezogener Daten".

Mit der Änderung soll künftig direkt auf die Verordnung (EU) 2016/679 verwiesen und der dort gewählte Überbegriff verwendet werden.

**Zu Artikel 25
Thüringer Bestattungsgesetz**

Es handelt sich bei der Änderung des § 15 Abs. 4 Satz 2 um eine redaktionelle Anpassung der Verweise ins Thüringer Datenschutzgesetz infolge der Umsetzung der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72). Die Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken ist stets vereinbar mit dem ursprünglichen Zweck der Datenverarbeitung, Artikel 5 Abs. 1 Buchst. b der Verordnung (EU) 2016/679.

**Zu Artikel 26
Änderung des Thüringer Laufbahngesetzes
Zu Nummer 1 (§ 25 Abs.1)**

Es handelt sich um eine redaktionelle Anpassung.

Zu Nummer 2 (§ 25 Abs. 4)

Es handelt sich um eine redaktionelle Anpassung an die Begriffsbestimmungen der Verordnung (EU) 2016/679.

**Zu Artikel 27
Inkrafttreten, Außerkrafttreten**

Artikel 27 regelt in Absatz 1 das Inkrafttreten des Gesetzes. Gleichzeitig mit dem Inkrafttreten des Mantelgesetzes tritt nach Absatz 2 das derzeit geltende Thüringer Datenschutzgesetz außer Kraft.

Zu Absatz 1:

Da durch Artikel 1 dieses Gesetzes die Verordnung (EU) 2016/679 umgesetzt wird und diese nach Artikel 99 der Verordnung (EU) 2016/679 ab dem 25. Mai 2018 unmittelbar gilt, sind bis zu diesem Datum sämtliche nationalen Datenschutzgesetze an deren Vorgaben anzupassen.

Zu Absatz 2:

Gleichzeitig tritt das geltende Thüringer Datenschutzgesetz außer Kraft, da die Verordnung (EU) 2016/679 unmittelbar gilt und die noch erforderlichen beziehungsweise möglichen ergänzenden Regelungen durch Artikel 1 im neuen Thüringer Datenschutzgesetz getroffen werden. Bisherige datenschutzrechtliche Standards und wesentliche Regelungen entfallen dabei durch die neue Regelungssystematik nicht. Vielmehr finden sich die in Ergänzung zur Verordnung (EU) 2016/679 und zur Beibehaltung bisheriger Thüringer Regelungen getroffenen Bestimmungen im neuen Thüringer Datenschutzgesetz. Zum anderen ergeben sich bisherige Bestimmungen des Thüringer Datenschutzrechts nunmehr unmittelbar aus der Verordnung (EU) 2016/679.