

Der Regierungsrat des Kantons Thurgau an den Grossen Rat

Frauenfeld, 23. September 2025
Nr. 501

EINGANG GR		
29.9.25		
24	GE 10	206

Botschaft zur Änderung des Gesetzes über den Datenschutz (TG DSG) und des Gesetzes über das Einwohnerregister sowie kantonale Register (ErG)

Sehr geehrter Herr Präsident
Sehr geehrte Damen und Herren

Wir unterbreiten Ihnen Botschaft und Entwurf zur Änderung des Gesetzes über den Datenschutz (TG DSG; RB 170.7) und des Gesetzes über das Einwohnerregister sowie kantonale Register (ErG; RB 142.15).

1. Ausgangslage

1.1. Umsetzung des internationalen Rechts auf kantonaler Ebene

Aufgrund des raschen technischen Fortschritts kommt dem Datenschutz eine immer wichtigere Rolle zu. Dies hat dazu geführt, dass auf dem europäischen Kontinent diverse neue Regelungen zum Datenschutz erlassen wurden. Diese sind von der Schweiz und den Kantonen in das eigene Recht zu übernehmen.

1.1.1. Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016

Die Europäische Union (EU) hat die Datenschutzgesetzgebung erneuert. Aufgrund des Schengen-Assoziierungsabkommens (SAA; SR 0.362.31) muss die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck 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 von der Schweiz und den Kantonen in das eigene Recht übernommen werden.

Das SAA erleichtert den Reiseverkehr zwischen der Schweiz und den Mitgliedsstaaten der EU. Die Personenkontrollen an den Binnengrenzen sind grundsätzlich aufgehoben worden. Demgegenüber wurden polizeiliche Ausgleichsmassnahmen zur Stärkung der inneren Sicherheit eingeführt. Die in diesem Zusammenhang vom Europäischen Parlament und Rat erlassene Richtlinie (EU) 2016/680 ist von der Schweiz und allen Kantonen zwingend umzusetzen.

1.1.2. Konvention 108 und Konvention 108+

Der Europarat hat das Übereinkommen des Europarates zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Konvention 108) durch das zweite Änderungsprotokoll zum Übereinkommen (Konvention 108+) ratifiziert und am 10. Oktober 2018 zur Unterzeichnung aufgelegt. Die Schweiz hat das Änderungsprotokoll zum Übereinkommen des Europarates zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten (Konvention 108+) am 21. November 2019 unterzeichnet und am 7. September 2023 ratifiziert. Die Konvention 108+ tritt in Kraft, wenn 38 Vertragsstaaten das Änderungsprotokoll ratifiziert haben. Ab dem Inkrafttreten der Konvention 108+ ist diese für die Schweiz und alle Kantone zwingend umzusetzen. Der Text der ratifizierten Konvention 108+ wird daher im aktuellen Revisionsverfahren des TG DSG berücksichtigt.

Bis zum Inkrafttreten der Konvention 108+ gelten die Vorgaben des Übereinkommens des Europarates zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28. Januar 1981 (Konvention 108), die in der aktuell geltenden Fassung des TG DSG bereits umgesetzt wurden.

1.1.3. Umsetzung in der Schweiz und den Kantonen

Aufgrund der internationalen Vorgaben hat die Schweiz das Bundesgesetz über den Datenschutz (DSG; SR 235.1) per 1. September 2023 angepasst. Die Kantone haben nun die internationalen Vorgaben ebenfalls umzusetzen. Das Gesetz über den Datenschutz des Kantons Thurgau ist deshalb zwingend an die Richtlinie (EU) 2016/680 anzupassen. Im Bereich der Konvention 108+ ist der Änderungsbedarf ebenfalls erwünscht, da sie von der Schweiz am 21. November 2019 unterzeichnet und am 7. September 2023 ratifiziert wurde und in Kraft treten wird, sobald 38 Vertragsstaaten das Änderungsprotokoll ratifiziert haben.

Neben der Umsetzung der internationalen Vorgaben werden nur noch einzelne, marginale Anpassungen vorgenommen. Die meisten Änderungen des TG DSG sind schengenrelevant und müssen aufgrund internationaler Verpflichtungen übernommen werden.

1.2. Anpassung der kantonalen Gesetzgebung

Im Bereich des Datenschutzes ist das Bundesrecht nicht übergeordnet. Die Kantone erlassen eigene Regelungen zur Bearbeitung von Personendaten durch die Behörden im eigenen Kanton. Jedoch sind die Kantone verpflichtet, die internationalen Vorgaben umzusetzen.

Mit der Revision des TG DSG ist für die Politischen Gemeinden kein eigener gesetzlicher Regelungsbedarf verbunden. Sowohl die Politischen Gemeinden als auch die Schulgemeinden unterstehen dem TG DSG, weshalb die Anpassung des TG DSG zu keinen rechtlichen Anpassungen auf kommunaler Ebene führen wird.

2. Finanzielle Auswirkungen

Die Revision des TG DSG wird höchstens kurzfristig finanzielle oder personelle Auswirkungen für die Gemeinden haben. Neben einem anfänglichen Schulungsbedarf und der internen Überprüfung der eigenen faktischen Verhältnisse an die neuen Vorgaben ist mit keinen mittel- oder langfristigen Mehrkosten zu rechnen.

Aus der geplanten Vorlage ergeben sich für den Kanton keine finanziellen und personellen Auswirkungen. Es werden keine neuen Stellen benötigt, insbesondere werden, entgegen der bundesrechtlichen Lösung, in den Departementen und der Staatskanzlei keine neuen Stellen für Datenschutzberaterinnen oder -berater zu besetzen sein. Dies wird vom übergeordneten Recht nicht verlangt und deshalb in der laufenden Revision auch nicht umgesetzt. Somit sind höchstens die Stellenbeschreibungen in der Aufsichtsstelle Datenschutz und Öffentlichkeitsprinzip an die neuen Funktionen anzupassen. Auch im Bereich der Arbeitsmittel wird kein Änderungsbedarf anfallen.

Die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung wird anfangs zu einem gewissen Mehraufwand (insbesondere Schulung) bei den öffentlichen Organen führen. Das neue Instrument der Datenschutz-Folgenabschätzung wird jedoch mittel- und langfristig zu einem Minderaufwand für neue Digitalisierungsprojekte führen, soweit durch geeignete Massnahmen die Sicherheit und der Datenschutz gewährleistet werden kann. Dies ist der Fall, weil bei diversen Projekten bereits in einem frühen Stadium erkannt werden kann, dass keine hohen Risiken für die Grundrechte der betroffenen Personen bestehen werden, womit diese Projekte keiner weiteren Prüfung unterzogen werden müssen. Diverse Digitalisierungsprojekte können dadurch rascher verwirklicht werden, was zu Kosteneinsparungen führen wird.

Durch die neue Informationspflicht bei der Beschaffung von Personendaten kann ein weiterer Anfangsaufwand entstehen, der aber als gering zu beurteilen ist. Die Meldepflicht der öffentlichen Organe bei Datenschutzverletzungen wird schon heute aus dem

Grundsatz von Treu und Glauben abgeleitet und dürfte deshalb zu keinem Zusatzaufwand führen.

3. Vernehmlassungsverfahren

Mit RRB Nr. 558 vom 20. August 2024 ermächtigte der Regierungsrat das Departement für Justiz und Sicherheit (DJS) zur Durchführung eines externen Vernehmlassungsverfahrens. Die Vernehmlassung zur Teilrevision des TG DSG dauerte vom 26. August 2024 bis zum 26. November 2024. Insgesamt gingen 36 Vernehmlassungsantworten zur vorgeschlagenen Gesetzesrevision ein. Es äusserten sich fünf kantonale Parteien, 15 Politische Gemeinden, fünf Schulgemeinden, der Verband Thurgauer Gemeinden (VTG) und der Verband Thurgauer Schulgemeinden (VTGS), die evangelische Landeskirche des Kantons Thurgau, sieben kantonale Stellen sowie ein Gericht. Sämtliche Stellungnahmen begrüssen ausdrücklich oder stillschweigend die Vernehmlassungsvorlage.

Die Auswertung der Vernehmlassungsantworten hat verschiedene berechtigte Anliegen aufgezeigt, die zu einer Anpassung der Vorlage zum TG DSG geführt haben:

- Da es sich bei § 3 Abs. 2 Ziff. 3 und Ziff. 6 um Wiederholungen handelt, erfolgen nachfolgende Änderungen:
Ziff. 3: die Gesundheit und Intimsphäre
Ziff. 6: das Erbgut (genetische Daten) oder die ethnische Herkunft.
- Im Klammervermerk von § 3 Abs. 2 Ziff. 8 soll lediglich das Profiling erwähnt werden (ohne den Zusatz „mit hohem Risiko“).
- § 3 Abs. 5 wird wie folgt angepasst:
Profiling ist jede, insbesondere automatisierte, Auswertung von Personendaten, um bestimmte persönliche Aspekte, die sich auf eine Person beziehen, zu bewerten oder persönliche Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten oder Aufenthaltsort.
- Trotz einiger kritischer Rückmeldungen im Vernehmlassungsverfahren soll das hohe Risiko in § 7a Abs. 2 nicht auf Gesetzesstufe definiert werden. Die Risiken ändern sich aufgrund der rasch fortschreitenden Technik sehr schnell. Die Aufzählung von Risiken, wie sie der Bund im DSG vornimmt, kann dazu führen, dass das TG DSG schon bald wieder an die neuen Verhältnisse angepasst werden müsste (vgl. Aufzählung in Art. 22 Abs. 2 DSG).
- Die Vernehmlassungsteilnehmenden kritisierten teilweise, dass der Titel von § 7b unklar formuliert sei und zu Verwechslungen führen könnte. Es sei nicht klar, ob beispielsweise Gemeinden den Datenschutz- und Öffentlichkeitsbeauftragten oder

die Aufsichtsstelle gemäss § 17 zu konsultieren haben. Der Titel wird deshalb klarer formuliert und lautet nun: Konsultation der Aufsichtsstellen.

- Zu § 17 wurde angeregt, dass nicht nur andere Gemeinden, sondern auch andere externe Stellen (z.B. eine Anwältin oder ein Anwalt) die Stellvertretungsfunktion übernehmen könnten. Zudem wurde beantragt, das Wort „drohende“ in „potentielle“ zu ändern, was einer Stärkung der Gemeinden entspräche. Diese Vorschläge sind zu begrüßen. Der Gesetzestext von § 17 Abs. 3 wird entsprechend angepasst.
- Von den Vernehmlassungsteilnehmenden wurde vorgebracht, dass die Bestimmung des § 21 Abs. 2 paternalistisch sei. Jede Person müsse selbst entscheiden, ob sie durch die Einsichtnahme belastet werde. Der Staat könne diese Entscheidung nicht treffen. Allenfalls könne der Staat darauf hinweisen, dass Informationen belastend sein könnten. Beim Auskunftsrecht handelt es sich um ein höchstpersönliches Recht, das nicht übertragbar ist und grundsätzlich nur von der betroffenen Person selbst geltend gemacht werden kann. Die gesuchstellende Person kann sich aber nach Beauftragung einer Vertreterin oder eines Vertreters zur Beantragung von Einsicht in die Daten vertreten lassen. Im Hinblick auf die bestehenden bundesrechtlichen Vorschriften ist eine kantonale Regelung der Stellvertretung nicht erforderlich, so dass § 21 Abs. 2 aufgehoben wird.

Zur Präzisierung wurden ausserdem die folgenden Aspekte vorgeschlagen, die jedoch nicht berücksichtigt wurden, weil die Änderungen des TG DSG entweder auf Vorgaben aus übergeordnetem Recht beruhen oder für die vorgebrachten Änderungsvorschläge keine sachlich überzeugenden Gründe für eine Aufnahme ins Gesetz vorliegen:

- Es wurde teilweise beantragt, dass sich die Aufsicht beim privatrechtlichen Handeln öffentlicher Organe nach dem Bundesrecht richten solle. Damit läge die Zuständigkeit beim Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). In § 2 Abs. 3 Satz 1 ist bereits geregelt, dass das kantonale Datenschutzgesetz bei privatrechtlicher Tätigkeit keine Anwendung findet. In § 2 Abs. 3 Satz 2 wird lediglich konkretisiert, was bereits heute gilt: Beim privatwirtschaftlichen Handeln öffentlicher Organe gelten die entsprechenden Regeln des Bundes, die Aufsicht richtet sich demgegenüber nach kantonalem Recht.
- Im Weiteren wurde unter Bezugnahme auf das Gesetz über Aktenführung und Archivierung (ArchivG; RB 432.10) sowie auf das Gesetz über das Öffentlichkeitsprinzip (Öffentlichkeitsgesetz, ÖffG; RB 170.6) angeregt, den Titel von § 2 in „Sachlicher Geltungsbereich“ zu ändern und einen neuen § 2^{bis} „Zeitlicher Geltungsbereich“ einzufügen, der Fristen regelt, wie lange Personendaten dem TG DSG unterstellt sind. Obwohl in der Praxis eine gewisse Unsicherheit bezüglich Aufbewahrungs- und Löschrufen bestehen, wäre eine Abkehr von der bisherigen

bewährten Praxis und Festlegung auf Gesetzesstufe nicht ratsam, da sich die Bestimmung einer Frist aufgrund verschiedener Ausnahmetatbeständen als schwierig erweisen würde (z.B. bei der Löschung von Covid-19 Personendaten). Zudem bestehen im zeitlichen Anwendungsbereich des TG DSG die Abgrenzungsschwierigkeiten nicht, wie sie sich beim zeitlichen Geltungsbereich des ArchivG und des ÖffG ergeben haben. Mit Blick auf das DSG, das keine Regelung zum zeitlichen Geltungsbereich getroffen hat, sowie mit Blick auf § 1 TG DSG, der den Zweck des Gesetzes – die Regelung der Bearbeitung von Personendaten zum Schutz der Persönlichkeit – festlegt, ist die Normierung eines zeitlichen Geltungsbereiches und damit die Änderung des TG DSG nicht angezeigt.

- Im Gegensatz zu den internationalen Vorgaben sowie zum DSG wird am Schutz juristischer Personen festgehalten (§ 3 Abs. 1). Dies hat in der Vernehmlassung teilweise zu Kritik geführt. Dennoch wird dieser Punkt beibehalten. Eine Aufhebung der Anwendbarkeit des TG DSG auf die Daten juristischer Personen hätte zur Folge, dass sämtliche Gesetzesgrundlagen, welche die Bearbeitung von Personendaten regeln, auf juristische Personen nicht mehr anwendbar wären und allenfalls angepasst werden müssten.
- Ferner wurde angeregt, die Begriffe in § 3 aus dem Bundesrecht zu übernehmen. Die Übernahme aller Begriffe des Bundesrechts stellt eine unpassende Einschränkung dar. Die Kantone sind frei, die Begriffe selbst zu definieren. Wird die Liste der besonders schützenswerten Personendaten zu stark eingeschränkt, besteht die Gefahr, dass die kantonale Gesetzgebung zu diesen sensiblen Daten gerichtlich korrigiert wird. Es empfiehlt sich deshalb, die kantonalen Regelungen möglichst offen zu gestalten, was sich im Kanton Thurgau bewährt hat.
- Es wurde beantragt, die Möglichkeit des Widerrufs gemäss § 4 Abs. 4 zu streichen. Daran wird festgehalten. Eine betroffene Person soll die Möglichkeit haben, die ausdrücklich erteilte Zustimmung zu widerrufen und dadurch dem öffentlichen Organ die Bearbeitung von Personendaten zu untersagen. Zudem sind Einwilligungen im Datenschutz bereits heute immer widerrufbar.
- Für § 4 wurde ein neuer Abs. 5 beantragt, der den Austausch zwingend benötigter Daten zwischen mit öffentlichen Aufgaben betrauten Organen erlaubt. Ein solcher Absatz wäre zu wenig konkret. Es ist nicht klar, welche Behörden welche Personendaten austauschen dürften. Vielmehr wäre und ist dies in den Spezialgesetzen zu regeln.
- Obwohl § 6 inhaltlich keine Änderung erfährt, sind dazu einzelne Rückmeldungen eingegangen. Es wurde kritisiert, dass die Verantwortlichkeit bei gemeinsamen Datensammlungen nicht klar geregelt sei. In der Praxis kommt die Verantwortung den Leitungsorganen in ihrem Zuständigkeitsbereich zu. Sind mehrere Behörden an einer Bearbeitung beteiligt, haben sie einander die Verantwortung transparent zuzuweisen. Oft kann die Verantwortung auch zwingend aus Spezialgesetzen

oder Verordnungen entnommen werden, aus denen sich bei der gemeinsamen Datenbearbeitung ein Über- oder Unterordnungsverhältnis herauslesen lässt.

- Es wurde teilweise gefordert, § 7a zu streichen oder zumindest stark einzuschränken, da befürchtet werde, dass die Datenschutz-Folgenabschätzung einen erheblichen Mehraufwand für die öffentlichen Organe bedeuten könnte oder Innovationen oder die Digitalisierung behindert werde. Die übergeordneten Rechtsgrundlagen (Art. 27 der Richtlinie [EU] 2016/680) verlangen eine Datenschutz-Folgenabschätzung durch das verantwortliche öffentliche Organ (vgl. ebenso: Art. 35 Verordnung [EU] 2016/679 [Datenschutz-Grundverordnung, EU-DSGVO], Art. 22 DSG). An die Risikobeurteilung werden keine hohen formellen Anforderungen gestellt. So kann in einem neuen Projekt bereits eine einfache Aktennotiz genügen, sofern keine hohen Risiken für die betroffenen Personen bestehen und folglich keine formellen Vorabkontrollen durchgeführt werden müssen. Bereits im bisherigen Recht war eine solche Kontrolle angezeigt, wenn die Bearbeitung von Personendaten besondere Risiken für die Rechte und Freiheiten der betroffenen Personen beinhalten kann. Eine Änderung von § 7a ist deshalb abzulehnen.
- Es wurde teilweise gefordert, die Grundzüge der Kriterien für die Bearbeitungsvorgänge in § 7b Abs. 3 festzulegen. Eine Normierung der Kriterien für Bearbeitungsvorgänge ist nicht sinnvoll, da diese offen formuliert werden sollen, damit auch künftige Vorgänge erfasst werden können.
- Einzelne Gemeinden teilten mit, dass die Frist von zwei Monaten in § 7b Abs. 2 weder sinnvoll noch umsetzbar sei. § 7b Abs. 2 lehnt sich an die bundesrechtliche Regelung an und soll deshalb sowohl für Gemeinden als auch für den Kanton verbindlich sein. Es ist davon auszugehen, dass mit dieser Regelung diverse Informatikprojekte rascher umgesetzt werden können, was zu begrüßen ist (vgl. Art. 23 DSG).
- Zu § 7c wurde kritisiert, dass die betroffenen Personen nicht nur über den automatisierten Entscheid, sondern auch über die zugrundeliegenden Kriterien und Datenquellen informiert werden müssten. Teilweise wurde gefordert, diesen Paragraphen ersatzlos zu streichen, da es unlogisch sei, dass in der heutigen Zeit der Digitalisierung und Automatisierung noch eine natürliche Person eine Überprüfung vornehme. Die Streichung ist problematisch: Künstliche Intelligenz ist stets abhängig von der eigenen Programmierung und vom antrainierten oder selbst beschafften Datenbestand. Die daraus resultierenden Entscheide können von den gesetzlichen Vorgaben oder vom gesunden Menschenverstand abweichen. Es ist deshalb wichtig, dass automatisierte Einzelfallentscheide, d.h. automatisierte, individuell konkrete Erlasse, entsprechend gekennzeichnet werden und die betroffenen Personen immer die Möglichkeit erhalten, dass die Entscheide (auf Verlangen) von einer natürlichen Person überprüft werden. Dies gewährleistet, dass dem Anliegen

aus dem Vernehmlassungsverfahren entsprochen wird. Automatisierte Einzelfallentscheide sollen nicht verboten werden. Es soll einzig die Möglichkeit der Überprüfung durch einen Menschen geschaffen werden. Deshalb wird von einer Änderung der Vorlage abgesehen.

- Es wurde beantragt, die Bestimmung betreffend Open Government Data (OGD) in § 11 Abs. 1^{bis} dahingehend zu ändern, dass die Rahmenbedingungen für OGD transparent dargelegt, aber keine allumfassende Pflicht für öffentliche Organe eingeführt werde, OGD aktiv und ohne Rücksicht auf Nutzen und Verhältnismässigkeit zu betreiben. Sollte an einer Pflicht für öffentliche Organe zur aktiven Bereitstellung von Daten festgehalten werden, so seien die Kriterien unter Berücksichtigung eines angemessenen Kosten-Nutzen-Verhältnisses auf Gesetzesstufe festzuhalten. Die Regelung ist bereits dahingehend gemindert, dass durch weitere Bestimmungen eingeschränkt werden kann, dass gewisse Daten zur Verfügung gestellt werden müssen. Zudem ist in der Vorlage bereits enthalten, dass der Regierungsrat ergänzende Vorschriften zum Einsatz von OGD erlassen darf, was mit der Open Government Data Verordnung vom 20. Mai 2025 (OGDV; RB 170.72) bereits erfolgt ist. Deshalb wird keine Änderung am § 11 Abs. 1^{bis} vorgenommen.
- Es wurde teilweise bemängelt, dass mit § 12 Abs. 1 der Beizug von Dienstleistern unnötig erschwert werde und die geltende Vorschrift die Pflichten bereits ausreichend und abschliessend regle. Zudem sei der Detaillierungsgrad zu hoch. Hier gilt es jedoch zu beachten, dass die internationalen Rechtsgrundlagen eine klare Zuordnung der Verantwortung für Datenbearbeitungen verlangen. Insbesondere wird verlangt, dass das öffentliche Organ gegenüber der Aufsichtsstelle nachweisen kann, dass es die Datenschutzbestimmungen bei der Auftragsdatenbearbeitung einhält. Der neu formulierte § 12 setzt diese Anforderungen um (Art. 22 Richtlinie [EU]2016/680) und kann deshalb nicht geändert werden.
- Es wurde beantragt, § 13 Abs. 2 ersatzlos zu streichen. Da im Kanton Thurgau kein Informationssicherheitsgesetz besteht, werden die Schutzziele an dieser Stelle normiert. Wenn der Kanton Thurgau ein eigenes Informationssicherheitsgesetz erlassen würde, müsste er die bundesrechtlichen Vorgaben (bei der Verwendung von Bundestools und Bundesdaten) nicht einhalten, sondern könnte eine angemessene eigene Regelung vorschlagen. Da aber ein solches Gesetz im Kanton Thurgau nicht geplant ist, empfiehlt es sich, wenigstens die grundlegenden Anforderungen an die Sicherheit im Datenschutzgesetz zu regeln, weshalb keine Änderung vorgenommen wird.
- Bei § 13b wurde kritisiert, dass er überflüssig sei oder zumindest schlanker gestaltet werden sollte. Die Informationspflicht ist eine Vorgabe aus übergeordnetem Recht (Art. 13 und Art. 14 Richtlinie [EU] 2016/680, Art. 8 Konvention 108+). Zu-

dem sollte sich der Aufwand für die öffentlichen Organe in einem vernünftigen Aufwand halten, weil die Informationspflicht entfällt, wenn das Bearbeiten der Personendaten gesetzlich vorgesehen ist. Dies wird in den meisten Fällen so sein. Deshalb wird an diesem Paragraphen festgehalten.

- Es wurde beantragt, § 13c ersatzlos zu streichen oder den Zusatz in Abs. 2: „die voraussichtlich zu einem Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt“ wegzulassen. Da es sich hier um eine Vorgabe aus übergeordnetem Recht handelt (Art. 30 f. Richtlinie [EU] 2016/680, Art. 7 Konvention 108+ und [nicht zwingend] Art. 24 DSG), ist an diesem Paragraphen festzuhalten. Auch aus Sicht der betroffenen Person ist es sinnvoll, Datenschutzverletzungen umgehend zu melden, da damit die Folgen allfälliger Datenschutzverletzungen minimiert werden können. Aufgrund der Meldung kann anschliessend beurteilt werden, ob und gegebenenfalls welche weiteren Massnahmen zielführend ergriffen werden müssen. Das öffentliche Organ muss eine Prognose über die möglichen Auswirkungen der Verletzung für die betroffene Person stellen. Nur wenn die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, ist eine Meldung obligatorisch.
- Es wurde zudem angeregt, die Anforderungen an die Aufsichtsstelle der Gemeinden zu spezifizieren. Dem ist entgegenzuhalten, dass die Gemeinden frei sein sollen, die Anforderungen an ihre Aufsichtsstelle selbst festzulegen. Dabei müssen sie die internationalen Vorgaben einhalten und sich bei etwaigen Änderungen mindestens an die Vorgaben der geplanten Revision des TG DSG halten. Auf eine Anpassung wird daher verzichtet.
- Gemäss § 18b kann der oder die Datenschutz- und Öffentlichkeitsbeauftragte den öffentlichen Organen Empfehlungen zur Bearbeitung von Personendaten geben. Sofern ein öffentliches Organ erklärt, der Empfehlung nicht folgen zu wollen oder ihr tatsächlich nicht folgt, kann der oder die Datenschutz- und Öffentlichkeitsbeauftragte die Empfehlung oder Teile davon gestützt auf § 18b Abs. 3 und § 18 Abs. 4 in der Form eines Entscheids erlassen. Es wurde teilweise von den Vernehmlassungsteilnehmenden beantragt, diese Verfügungsbefugnis zu streichen. Es sei eine massive Machtausweitung des oder der Datenschutz- und Öffentlichkeitsbeauftragten. Es wurde bemängelt, dass entweder eine Empfehlung oder eine Verfügung erlassen werden könne, beides sei Augenwischerei. Zudem sei es nicht zielführend und werde als Misstrauensvotum gegenüber den öffentlichen Organen verstanden. Gemäss den völkerrechtlichen Vorgaben muss die Aufsichtsstelle die Möglichkeit haben, Entscheide auszustellen und die Verantwortlichen anzuweisen, Verarbeitungsvorgänge, gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums, mit den nach dieser Richtlinie erlassenen Vorschriften in

10/31

Einklang zu bringen (Art. 47 Richtlinie [EU] 216/680 und Europarat: Art. 12 Konvention 108+, Art. 50 f. DSG). Aufgrund des Wortlauts der entsprechenden Bestimmungen muss der Aufsichtsstelle dieses Recht zwingend zustehen.

- Es wurde kritisiert, dass die Möglichkeit der aufsichtsrechtlichen Anzeige bereits im Gesetz über die Verwaltungsrechtspflege (VRG; RB 170.1) geregelt und dass § 23b deshalb überflüssig sei. Die in § 74 und § 75 VRG geregelte Anzeige unterscheidet sich von der aufsichtsrechtlichen Anzeige nach § 23b dadurch, dass im Rahmen des VRG jedermann jederzeit der Aufsichtsbehörde (vermeintliche) Missstände zur Kenntnis bringen kann, während im TG DSG eine betroffene Person bezüglich ihrer eigenen Personendaten handelt. Die Rechtsfolgen sind unterschiedlich (vgl. Informationspflicht). Auf das Anliegen wird deshalb nicht eingegangen.
- Es wurde angeregt, eine Stelle zu schaffen, um im Bereich des Datenschutzes Beratungen durchzuführen und Hilfestellung zu Einsichtnahme und Auskunftserteilung zu geben (§ 23c). Dies wird damit begründet, dass viele Personen nicht ihre Rechte und die Möglichkeiten zur Einsichtnahme kennen würden. Dem ist entgegenzuhalten, dass gemäss § 18 Abs. 1 Ziff. 2 der oder die Datenschutz- und Öffentlichkeitsbeauftragte bereits betroffene Personen über ihre Rechte berät. Diese Möglichkeit wird rege in Anspruch genommen. Die Schaffung einer zusätzlichen Beratungsstelle ist daher abzulehnen.

Darüber hinaus wurde von den Vernehmlassungsteilnehmenden vorgebracht, dass einige Paragraphen des bisherigen Rechts, die nicht Gegenstand der Revision und des Vernehmlassungsverfahrens waren, kantonalen Bestimmungen widersprechen würden. Folgende Anliegen führten im Ergebnis zu einer Anpassung des Gesetzes:

- Es wurde vorgebracht, § 14 Abs. 1 widerspreche den Vorschriften des ArchivG. Da das öffentliche Organ gemäss § 12 Abs. 1 ArchivG die Akten auf der Grundlage des Registraturplans zu führen hat, wird zur Vermeidung widersprüchlicher gesetzlicher Normen § 14 wie folgt angepasst:

Abs. 1: Das verantwortliche Organ führt entsprechend der Vorgaben des Gesetzes über Aktenführung und Archivierung (ArchivG) ein Register über die von ihm angelegten Datensammlungen.

- Ferner wurde aufgeworfen, § 14 Abs. 3 widerspreche den Vorschriften des ArchivG, insbesondere der im ArchivG geregelten Aktenführung (§ 12) und Bewertung (§ 13), da das Staatsarchiv in Absprache mit dem öffentlichen Organ die Archivwürdigkeit von Akten und Unterlagen bewerte. Demgegenüber sehe Art. 14 Abs. 3 vor, dass das verantwortliche Organ allein, das heisst ohne Absprache mit dem Staatsarchiv, darüber entscheiden könne, welche Datensammlungen in das Register aufgenommen oder ausgeschlossen werden. Zur Vermeidung widersprüchlicher gesetzlicher Normen wird § 14 Abs. 3 aufgehoben. Zudem ist eine

kantonale Regelung, insbesondere § 14 Abs. 3 Ziff. 3, nicht erforderlich, da für die Datenbearbeitung, Aktenführung und Aktenaufbewahrung durch die Strafverfolgungsbehörden gestützt auf Art. 99 ff. der Schweizerischen Strafprozessordnung (Strafprozessordnung, StPO; SR 312.0) spezialgesetzliche Regelungen bestehen.

- Des Weiteren wurde vorgebracht, dass § 16 Abs. 1 mit dem ArchivG in Konflikt stehe, da die Vernichtung von Datensammlungen erst nach Ablauf der Aufbewahrungsfristen sowie nach Bewertung durch das Staatsarchiv in Absprache mit dem öffentlichen Organ als archivwürdig erfolgen könne (§ 13 Abs. 1 i.V.m. § 15 Abs. 1 ArchivG). Diesem Vorbringen ist der Vorbehalt gemäss § 16 Abs. 2 entgegenzuhalten, der auf die Vorschriften des ArchivG verweist. Da Rechtsnormen so zu formulieren sind, dass ihr Inhalt eindeutig ist, wird § 16 Abs. 1 zur Klarstellung wie folgt gefasst und gleichzeitig auf Abs. 2 verzichtet:

Abs. 1: Das verantwortliche Organ legt in Absprache mit dem Staatsarchiv und unter Berücksichtigung der Vorgaben des ArchivG für jede Datensammlung fest, wann Personendaten zu vernichten oder zu archivieren sind.

Abs. 2: aufgehoben.

4. Erläuterungen zu den einzelnen Bestimmungen

§ 2 Abs. 2 (geändert)

Zur besseren Verständlichkeit wird der Begriff des „Staates“ durch den Begriff des „Kantons“ ersetzt. Zudem wird der Begriff des „Beamten“ entfernt, da im Kanton Thurgau der Beamtenstatus schon im Jahr 2001 durch eine entsprechende Verfassungsänderung aufgehoben worden ist. Eine inhaltliche Änderung findet indessen nicht statt. Es handelt sich um eine redaktionelle Änderung ohne materiell-rechtliche Auswirkung.

§ 2 Abs. 3 (geändert)

Bereits nach geltendem Recht erstreckt sich der Geltungsbereich des TG DSG nicht auf die privatrechtliche Tätigkeit öffentlicher Organe. Soweit öffentliche Organe privatrechtlich handeln, soll das TG DSG weiterhin keine Anwendung finden. Mit der neuen Regelung in § 2 Abs. 3 soll die bestehende Unklarheit beseitigt und Missverständnisse vermieden werden.

Am wirtschaftlichen Wettbewerb nimmt ein öffentliches Organ teil, wenn es seine Leistungen auf dem Markt in Konkurrenz zu anderen Personen anbietet und mit seinem Handeln Gewinn erzielt. Das heisst, deren Vertragspartnerinnen und -partner müssen beim Vertragsabschluss frei sein, und ihre Rechte und Pflichten dürfen sich nicht aus einer Verfügung oder einem verwaltungsrechtlichen Vertrag ergeben (BEAT RUDIN, in:

RUDIN BEAT/BAERISWYL BRUNO [HRSG.], Praxiskommentar zum Informations- und Datenschutzgesetz des Kantons Basel-Stadt [IDG], Zürich - Basel - Genf 2014, § 2 N 13). Solche privatrechtlich handelnden Behörden werden dadurch nicht zu Privaten, sondern handeln lediglich wie Private und bleiben weiterhin öffentliche Organe. Die Lehre geht mehrheitlich davon aus, dass der EDÖB grundsätzlich nur die Aufsicht über Bundesorgane und Privatpersonen wahrnimmt. Kantonale und kommunale Organe unterstehen nicht seiner Aufsicht. Da es keinen aufsichtsfreien Raum geben kann, hat die Zuständigkeit bei der kantonalen oder kommunalen Aufsichtsstelle zu verbleiben.

Anzumerken ist, dass das kantonale Datenschutzgesetz für alle öffentlichen Organe gilt, unabhängig davon, ob sie Bundesrecht, kantonales Recht oder Recht von Gemeinden vollziehen. Die neue Regelung dient somit der Klarstellung der bereits bestehenden Regelung, ohne inhaltliche Änderungen vorzunehmen.

§ 2 Abs. 4 (geändert)

Um Überschneidungen zwischen den verfahrensrechtlichen und den datenschutzrechtlichen Informationsansprüchen der betroffenen Personen zu vermeiden, werden die Ansprüche während laufender Verfahren klarer geregelt. Demnach regelt das anwendbare Verfahrensrecht die Bearbeitung von Personendaten und die Rechte der betroffenen Personen in sämtlichen Verfahren vor Gerichtsbehörden und verwaltungsinternen Verwaltungsjustizbehörden. Auch allfällige spezialgesetzliche Bestimmungen ausserhalb der eigentlichen Verfahrensgesetze fallen unter den Begriff „anwendbares Verfahrensrecht“. Daraus ergibt sich, dass die Datenbearbeitung während hängiger Gerichts- oder Verwaltungsverfahren nicht der Aufsicht der Aufsichtsstelle Datenschutz- und Öffentlichkeitsprinzip unterstehen (vgl. ebenso in Art. 45 Richtlinie [EU] 2016/680, Art. 15 Konvention 108+, Art. 4 Abs. 2 DSG).

Die Formulierung von § 2 Abs. 4 orientiert sich weitgehend am Bundesgesetz (Art. 2 Abs. 3 DSG). Zusätzlich zur Regelung auf Bundesebene müssen im TG DSG die Verfahren der Verwaltungsrechtspflege erwähnt werden, in denen sich die Rechte und Pflichten der betroffenen Person während hängiger Verfahren nach dem VRG richten. In Verwaltungsverfahren (Verfahren auf Erlass einer Verfügung) gelten weiterhin die Bestimmungen des kantonalen Datenschutzgesetzes, weshalb die Verwaltungsbehörden nicht aufgeführt werden.

Im Umkehrschluss bedeutet dies, dass das kantonale Datenschutzrecht auf die Datenverarbeitung durch die administrativen Dienste von Gerichten und Verwaltungsrechtspflegebehörden, beispielsweise bei der Bearbeitung von Personaldaten, anwendbar ist.

Nach Abschluss des Verfahrens kommt wie bisher das TG DSG zur Anwendung (siehe Urteil des Obergerichts des Kantons Thurgau [OGer TG] vom 6. Juli 2023 im Verfahren SW.2023.61, elektronisch publiziert im Separatum zum Rechenschaftsbericht des OGer

TG an den Grossen Rat, abrufbar unter: <https://rechtsprechung.tg.ch/og/rbog-2023-nr-52>, RBOG 2023 Nr. 52), ausser es bestehen spezialgesetzliche Regelungen (z.B. § 69 Kindes- und Erwachsenenschutzverordnung [KESV; RB 211.24]).

§ 3 Abs. 1 (keine Änderung)

Das DSG gilt nur noch für den Schutz der Persönlichkeit von natürlichen Personen. Dies ist zu eng gefasst. Es können sich in der Praxis Konstellationen ergeben, bei denen die Daten von juristischen Personen weiterhin geschützt werden müssen. Der Schutz juristischer Personen ist deshalb nicht aufzuheben (anders Art. 1 DSG sowie Art. 1 der Verordnung [EU] 2016/679).

In der Vernehmlassung wurde teilweise kritisiert, dass das kantonale Recht in einzelnen Punkten vom Bundesrecht abweicht. Eine Teilnehmerin führte aus, dass die Rechte juristischer Personen auch ohne das TG DSG geschützt seien, beispielsweise durch das Schweizerische Zivilgesetzbuch (ZGB; SR 210) oder das Bundesgesetz gegen den unlauteren Wettbewerb (UWG; SR 241). Eine andere Teilnehmerin äusserte sich dahingehend, dass die Daten juristischer Personen durch Spezialgesetze auf nationaler Ebene ausreichend gewahrt seien und sich das TG DSG an den Entwicklungen auf internationaler und nationaler Ebene orientieren sollte.

Auch juristische Personen haben eine gesetzlich geschützte Privatsphäre. Eine Aufhebung der Anwendbarkeit des TG DSG auf die Daten juristischer Personen hätte aufgrund des Legalitätsprinzips zur Folge, dass sämtliche Regelungen des materiellen Datenschutzes die Daten juristischer Personen nicht mehr umfassen würden.

Bei einer Beschränkung des Geltungsbereichs auf natürliche Personen müssten alle Bestimmungen in der Gesetzessammlung des Kantons Thurgau überprüft werden, die sich auf „Personendaten“ beziehen, um festzustellen, ob sie auch für Daten juristischer Personen gelten sollen, und es müsste der Schutzbedarf für die Daten juristischer Personen festgelegt werden. Dies hat beim Bund und bei anderen Kantonen zur Schaffung neuer Gesetzesgrundlagen (z.B. im Regierungs- und Verwaltungsorganisationsgesetz [RVOG; SR 172.010]) geführt, die allerdings weitgehend mit den Regelungen des Datenschutzgesetzes übereinstimmen. Es besteht dabei die Gefahr von Rechtslücken. Die bestehende Regelung ist aufgrund des langjährigen Bestandes anwenderfreundlich und praxisgeprüft, sie sollte beibehalten werden.

Entfiele der Schutz juristischer Personen durch das TG DSG, führte dies beispielsweise zu der problematischen Konstellation, dass die Kontrollschilder vorbeifahrender Geschäftsfahrzeuge juristischer Personen ohne Einschränkungen erfasst und publiziert werden dürften, sofern eine Mitarbeiterin oder ein Mitarbeiter des Unternehmens das Fahrzeug führt. Führt die gleiche Person ein Privatfahrzeug, wären die umfassende Erfassung und Publikation des Kontrollschilts nicht mehr erlaubt. Entfiele der Schutz der

14/31

juristischen Personen, müsste diese Ungleichbehandlung durch andere Gesetzgebungsprojekte aufgehoben werden. Das revidierte TG DSG soll folglich auch weiterhin juristische Personen schützen, soweit die Behörden im Kanton Thurgau deren Daten bearbeiten.

§ 3 Abs. 2 (geändert)

Die Aufzählung der Kategorien von besonders schützenswerten Personendaten bleibt weiterhin offen formuliert und ist deshalb nicht abschliessend geregelt. Es wird aber klargestellt, dass gewisse Arten von neu möglich gewordenen Datenerhebungen – insbesondere im Bereich der Genetik oder der Biometrie und der Big-Data-Auswertung (Profiling) – nur vorgenommen werden dürfen, wenn es ein formelles Gesetz erlaubt (Art. 3 Richtlinie [EU] 2016/680, Art. 6 Konvention 108, Art. 5 DSG).

§ 3 Abs. 2 Ziff. 3 (geändert)

Einzelne Vernehmlassungsteilnehmende weisen darauf hin, dass § 3 Abs. 2 Ziff. 3 (seelischer, geistiger oder körperlicher Zustand) mit dem Begriff „Gesundheit“ gemäss § 2 Abs. 2 Ziff. 6 gleichzusetzen sei und dies deshalb eine Wiederholung darstellen würde. Angaben über die Gesundheit umfassen alle Informationen, die Rückschlüsse auf den körperlichen oder geistigen Gesundheitszustand einer Person erlauben. Das Bundesgericht unterscheidet nach der „Drei-Säulen-Theorie“ zwischen der Intim- oder Geheimsphäre, der Privatsphäre sowie der Öffentlichkeitsphäre (BGE 97 II 97 E. 3 S. 100 ff.; BGE 118 IV 41 E. 4 S. 45 ff.). Die Intimsphäre erfasst dabei alle auf die persönlichen Angelegenheiten der betroffenen Person bezogenen Informationen wie das Sexualleben, das der Kenntnis Dritten grundsätzlich entzogen bleiben soll, ausser die betroffene Person informiert selbst darüber. § 3 Abs. 2 Ziff. 3 wurde daher geändert in „die Gesundheit und Intimsphäre“. § 3 Abs. 2 Ziff. 6 wurde in „das Erbgut (genetische Daten) oder die ethnische Herkunft“ geändert.

§ 3 Abs. 2 Ziff. 6 (neu)

Neu gelten Angaben zum Erbgut (genetische Daten) als besonders schützenswerte Personendaten. Genetische Daten sind Informationen über das Erbgut einer Person, die durch eine genetische Untersuchung gewonnen werden; darin eingeschlossen ist auch das DNA-Profil (Art. 3 lit. k des Bundesgesetzes vom 8. Oktober 2004 über genetische Untersuchungen beim Menschen [GUMG; SR 810.12]). Im Einklang mit dem europäischen Recht und dem Bund wird der Begriff „Erbgut (genetische Daten)“ in Ziff. 6 aufgenommen (Art. 10 Richtlinie [EU] 216/680, Art. 6 Konvention 108+).

Verzichtet wird auf den Begriff „Rasse“, da dieser nicht mehr zeitgemäss ist (Art. 6 Konvention 108+ und Art. 5 lit. c. Ziff. 2 DSG, anders weiterhin noch in Art. 10 Richtlinie

[EU] 216/680). Dafür wird der Begriff „ethnische Herkunft“ neu in § 3 Abs. 2 Ziff. 6 aufgenommen. Mit ethnischer Herkunft ist die Zugehörigkeit zu einer Gruppe von Menschen gemeint, die sich aufgrund ihrer Kultur, Geschichte, Sprache, Sitten, Traditionen und Gebräuche als untereinander verbunden und dadurch als von der übrigen Bevölkerung differente Gemeinschaft erleben oder von der übrigen Bevölkerung als differente Gruppe wahrgenommen werden.

§ 3 Abs. 2 Ziff. 7 (neu)

Im Gegensatz zum DSG sieht der Entwurf des revidierten TG DSG in § 3 Abs. 2 Ziff. 7 vor, den Begriff „biometrische Daten“ genauer zu definieren. Unter biometrischen Daten werden Personendaten verstanden, die durch ein spezielles technisches Verfahren aus den physischen, physiologischen oder verhaltensspezifischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen. Es handelt sich dabei beispielsweise um einen digitalen Fingerabdruck, Gesichtsbilder, Bilder der Iris oder Aufnahmen der Stimme. Diese Daten müssen zwingend auf einem spezifischen technischen Verfahren beruhen, das die eindeutige Identifizierung oder Authentifizierung einer Person erlaubt (Botschaft DSG, BBI 2017 7020).

§ 3 Abs. 2 Ziff. 8 (neu)

Neu werden die Begriffe „Persönlichkeitsprofil“ und „Profiling“ in die Kategorie der besonders schützenswerten Personendaten aufgenommen. Damit gelten für das Profiling die Anforderungen, die an die Bearbeitung von besonders schützenswerten Personendaten gestellt werden. Insbesondere ist § 4 Abs. 4 zu beachten, der eine hinreichend bestimmte Regelung in einem formellen Gesetz verlangt.

Auf Bundesebene werden zwei Profilingvarianten unterschieden: Das Profiling und das Profiling mit hohem Risiko. Der Bundesgesetzgeber übernimmt in Art. 5 lit. f DSG die Legaldefinition des Begriffs „Profiling“ der Vorschrift des Art. 3 Ziff. 4 der Richtlinie (EU) 2016/680 und Art. 22 der Verordnung über den Datenschutz (DSV; SR 235.11). Der Begriff „Profiling mit hohem Risiko“ ist eine Schöpfung der eidgenössischen Räte; er wird in Art. 5 lit. g DSG definiert. Auch der Kanton Thurgau anerkennt, dass nicht jedes Profiling mit einem hohen Risiko für die betroffene Person verbunden ist. Die Vernehmlassungsvorlage sah eine entsprechende Einschränkung ähnlich der Bundeslösung vor, nämlich, dass nur Profilings mit besonderen Risiken für die betroffene Person eine qualifizierte Gesetzesgrundlage erfordern würden. Fällt ein Profiling nicht unter die Begriffsdefinition des kantonalen Datenschutzgesetzes (§ 3 Abs. 5), so gelten die allgemeinen Anforderungen an die gesetzliche Grundlage, wenn dabei Personendaten oder unter Umständen auch besonders schützenswerte Personendaten bearbeitet werden. Damit wird auch der Kritik in der Vernehmlassung begegnet, wonach es unklar sei, wann hohe

Risiken für ein Profiling vorlägen oder wie diese im Verhältnis zum Profiling mit hohem Risiko des Bundes stünde. Dies widerspricht nicht den europäischen Grundlagen, da sie nur bei besonders schützenswerten Personendaten verlangen, dass deren Bearbeitung für die öffentliche Aufgabe unbedingt erforderlich sein muss und folglich nur dafür qualifizierte Anforderungen gelten (Art. 10 Richtlinie [EU] 2016/680).

In § 3 Abs. 5 wird der Begriff „Profiling“ definiert. Am Begriff des Persönlichkeitsprofils soll festgehalten werden, da dieser auch in anderen Gesetzen verwendet wird und dort nicht eins zu eins durch das Profiling ersetzt werden kann (z.B. § 67 Abs. 2 des Polizeigesetzes [PolG; RB 551.1] oder § 28 Abs. 1 des Gesetzes über das Kantons- und Gemeindebürgerrecht [KBüG; 141.1]).

§ 3 Abs. 3 (geändert)

In § 3 Abs. 3 wird die Legaldefinition des Begriffs „Bearbeiten“ entsprechend den europäischen und bundesrechtlichen Vorgaben ergänzt (Art. 2 i.V.m. Art. 3 Ziff. 2 der Richtlinie [EU] 2016/680 betreffend „Verarbeitung“, Art. 2 lit. c der Konvention 108+ betreffend „automatische Verarbeitung“ sowie Art. 5 lit. d DSG betreffend „Bearbeiten“).

§ 3 Abs. 5 (neu)

Im Interesse der Verständlichkeit ist „Profiling“ in die Begriffsdefinitionen aufzunehmen. Wird das Profiling als zusätzliche Kategorie unter die besonders schützenswerten Personendaten aufgenommen (§ 3 Abs. 2 Ziff. 8), geltend die Anforderungen, die an die Bearbeitung von besonderen Personendaten gestellt werden, insbesondere § 4 Abs. 4, der eine hinreichend bestimmte Regelung in einem formellen Gesetz verlangt.

Beim Profiling handelt es sich um die Art, wie diverse Daten miteinander verknüpft werden. Hier handelt es sich nicht um eine neue Datenkategorie, sondern um die Art und Weise, wie Daten verarbeitet werden. Die technologische Entwicklung ermöglicht es heute in immer stärkerem Ausmass, Datenmengen automatisiert zu verarbeiten, zu kombinieren und zu analysieren, um beispielsweise Tendenzen feststellen zu können, die wiederum bestimmten Gruppen oder einzelnen Personen zugeordnet werden können. Aufgrund der heute erst in Ansätzen erkennbaren technologischen Entwicklungen sind an das Profiling hohe Anforderungen zu stellen. Zwar erscheint aktuell ein staatlicher „citizen score“, wie ihn China kennt, noch weitgehend unvorstellbar und mit unseren Grundrechten nicht vereinbar, aber die Auswertungstechnologie dazu besteht bereits. Es braucht deshalb klare gesetzliche Rahmenbedingungen, um die Persönlichkeit wirkungsvoll zu schützen. Deshalb ist es sinnvoll, nicht zwischen Profilingvarianten zu unterscheiden, sondern jegliches Profiling unter die Kategorie „besonders schützenswerte Personendaten“ zu stellen. Das Profiling wird deshalb in einem eigenen Absatz definiert (Art. 3 Ziff. 4 Richtlinie [EU] 2016/680, Art. 5 lit. f, lit. g DSG).

17/31

§ 3 Abs. 6 (neu)

§ 12 Abs. 1 sieht den Beizug einer Auftragsdatenbearbeiterin oder eines Auftragsdatenbearbeiters vor. In § 3 Abs. 6 wird deshalb eine Legaldefinition des Begriffs „Auftragsdatenbearbeiter“ aufgenommen.

§ 4 Abs. 1 (geändert)

Der veraltete Ausdruck „hierfür“ wird durch „dazu“ ersetzt. Inhaltlich ergeben sich dadurch keine Änderungen.

§ 4 Abs. 4 (geändert)

Das Profiling gilt als eine besonders risikobehaftete Art der Datenbearbeitung in Bezug auf die Persönlichkeits- oder Grundrechte der betroffenen Person. Für das Profiling gelten die gleichen Voraussetzungen wie für die Bearbeitung von besonders schützenswerten Personendaten. Deshalb ist für die Erstellung von Persönlichkeitsprofilen (Profiling) immer eine Regelung in einem formellen Gesetz erforderlich (Art. 3 Richtlinie [EU] 2016/680, Art. 5 DSGVO).

In Bezug auf das alte Recht ergeben sich einzelne Änderungen und Konkretisierungen. Profiling gilt neu als besonders schützenswerte Art der Datenbearbeitung (vgl. Erläuterungen zu § 3 Abs. 2 Ziff. 8). Deshalb ist eine Grundlage in einem Gesetz erforderlich. Zudem wird in Übereinstimmung mit der Regelung des Bundes ein Auffangtatbestand für Datenbearbeitungen geschaffen, die weder ein Profiling noch ein Persönlichkeitsprofil darstellen, aber aufgrund des Bearbeitungszwecks oder der Art und Weise der Bearbeitung dennoch zu einem schwerwiegenden Eingriff in die Grundrechte der betroffenen Person führen können.

In § 4 Abs. 4 wird die Möglichkeit des Widerrufs der ausdrücklich erteilten Zustimmung zur Bearbeitung besonders schützenswerter Personendaten und zum Profiling aufgenommen. Die betroffene Person muss unter bestimmten Voraussetzungen und im Einzelfall die Möglichkeit haben, dem öffentlichen Organ die Bearbeitung von Personendaten zu untersagen. Das könnte beispielsweise der Fall sein, wenn die betroffene Person zunächst eine Einwilligung zur Veröffentlichung eines Fotos erteilt hat, diese aber später widerrufen möchte.

Die Annahme einer konkludent erteilten Zustimmung ist nach dem heutigen Datenschutzverständnis problematisch und dürfte einer gerichtlichen Beurteilung nicht standhalten.

§ 6 Abs. 2 (geändert)

§ 6 erfährt keine inhaltliche, sondern lediglich eine redaktionelle Änderung. Der Gesetztext wird moderner, systematischer und einfacher lesbar gestaltet. Insbesondere wird die Bezeichnung „Stelle“ durch den im ÖffG verwendeten Begriff des „öffentlichen Organs“ ersetzt.

Einzelne Vernehmlassungsteilnehmende verlangten, die Verantwortlichkeiten bei gemeinsamen Datenbearbeitungen müssten klar geregelt werden. Die Zuweisung der datenschutzrechtlichen Verantwortlichkeit ist im Datenschutzrecht ein wichtiges Prinzip. Sind mehrere Behörden an einer Bearbeitung beteiligt, müssen sie einander ihre jeweilige Verantwortung transparent zuweisen. Oft ist die Verantwortlichkeit in Spezialgesetzen geregelt (z.B. Personen- und Objektregister, PEROB). Zudem ist es möglich, dass sich aus einem Spezialgesetz oder einer Verordnung ein Über- oder Unterordnungsverhältnis bei der gemeinsamen Datenbearbeitung herauslesen lässt.

§ 7a (Titel geändert)

Der Titel von § 7a wurde von „Vorabkontrolle“ in „Datenschutz-Folgenabschätzung“ geändert.

§ 7a Abs. 1 (geändert)

Die bisherige Vorabkontrolle wird neu durch eine Datenschutz-Folgenabschätzung ersetzt, in der das öffentliche Organ selbst zu beurteilen hat, ob die eigene Datenbearbeitung ein hohes Risiko für die Verletzung der Grundrechte der betroffenen Personen beinhaltet. Das Vorgehen zur Durchführung einer Datenschutz-Folgenabschätzung wird gesetzlich vorgegeben. Die Normierung soll eine Hilfe darstellen, damit die öffentlichen Organe wissen, wie die verlangten Prüfungen durchzuführen sind. Ebenso wird damit sichergestellt, dass Datenschutz-Folgenabschätzungen bei allen öffentlichen Organen einheitlich durchgeführt und die gewählten Bemessungskriterien über einen längeren Zeitraum Bestand haben werden (Art. 27 Richtlinie [EU] 2016/680, Art. 10 Ziff. 2 Konvention 108+, Art. 22 DSG).

Das Instrument der Datenschutz-Folgenabschätzung soll dazu dienen, Risiken für die betroffenen Personen bereits in frühen Projektphasen zu erkennen und Massnahmen zu deren Bewältigung zu definieren. Der Begriff „Vorhaben“ verdeutlicht, dass die Datenschutz-Folgenabschätzung vor der Bearbeitung von Personendaten erfolgt. Damit wird der Datenschutz präventiv gewährleistet, so dass spätere, kostenintensive Nachbesserungen vermieden werden können. Eine Abschätzung der Risiken einer geplanten Datenbearbeitung muss in jedem Fall durchgeführt werden. Dies dürfte anfänglich zu einem gewissen Aufwand bei jedem Datenbearbeitungsprojekt führen. Allerdings werden an diese Einschätzung keine übermässigen Anforderungen gestellt. Wenn bei einer

geplanten Datenverarbeitung keine besonderen Gefahren erkennbar sind und folglich keine besonderen Vorkehrungen erforderlich sind, kann dies im Projekt mit einer Aktennotiz dokumentiert werden. Geplante Projekte können so speditiver abgewickelt werden.

§ 7a Abs. 2 (neu)

Trotz der kritischen Rückmeldungen im Vernehmlassungsverfahren soll der Begriff des „hohen Risikos“ nicht auf Gesetzesstufe fixiert werden (vgl. im Gegensatz dazu Art. 22 Abs. 2 DSG). Hohe Risiken – insbesondere bei der Verwendung neuer Technologien – können sich aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung ergeben. Diese Einteilungen können sich aber rasch ändern. Beispielsweise können sich hohe Risiken auch bei der Bearbeitung einer grossen Zahl von Personendaten ergeben. Die öffentlichen Organe sollen sich bei der Beurteilung eines hohen Risikos auf bestehende oder durch die Aufsichtsstellen noch zu erarbeitende Risikoprüfungsvorgaben stützen können.

§ 7a Abs. 3 Ziff. 1 bis Ziff. 3 (neu)

Entsprechend den europäischen Vorgaben und der Regulierung des Bundes (vgl. Art. 27 Abs. 2 Richtlinie [EU] 2016/680, Art. 22 Abs. 2 DSG) muss die Datenschutz-Folgenabschätzung mindestens eine allgemeine Beschreibung der geplanten Bearbeitungsvorgänge (Ziff. 1) enthalten und eine Bewertung der Risiken für die Grundrechte der betroffenen Personen (Ziff. 2), eine Darstellung und Bewertung der geplanten Abhilfemassnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz der Grundrechte der betroffenen Personen sichergestellt und der Nachweis erbracht werden kann, dass die Datenschutzbestimmungen eingehalten werden (Ziff. 3).

Stellt das öffentliche Organ mittels Selbstkontrolle fest, dass bei einem Vorhaben ein hohes Risiko besteht, nimmt es formell eine Datenschutz-Folgenabschätzung vor. Mit den darin aufgezeigten, getroffenen oder noch zu treffenden Massnahmen sollen die negativen Auswirkungen einer Bearbeitung verhindert oder zumindest eingeschränkt werden. Darunter fallen beispielsweise die Beschränkung des Zugangs zu den Daten sowie weitere Massnahmen zur Gewährleistung der Datensicherheit.

§ 7b Titel (neu)

Die Vernehmlassungsteilnehmenden kritisierten teilweise, dass der Titel „Konsultation des Datenschutz- und Öffentlichkeitsbeauftragten“ unklar formuliert sei und deshalb Verwechslungen zulasse. Es sei nicht klar, ob Gemeinden den Datenschutz- und Öffentlichkeitsbeauftragten oder die Aufsichtsstelle gemäss § 17 zu konsultieren haben. Der Titel wird deshalb von „Konsultation des oder der Datenschutz- und Öffentlichkeitsbeauftragten“ in den Titel „Konsultation der Aufsichtsstellen“ geändert.

20/31

§ 7b Abs. 1 (neu)

Die zuständige Aufsichtsstelle muss konsultiert werden, wenn Rechtsetzungsprojekte den Datenschutz betreffen (Abs. 1 Ziff. 1) oder die Bearbeitung von Personendaten gemäss Datenschutz-Folgenabschätzung voraussichtlich zu einem hohen Risiko für die Grundrechte der betroffenen Personen gemäss § 7a Abs. 2 führen wird (Abs. 1 Ziff. 2). Soweit die öffentlichen Organe zum Ergebnis gelangen, dass kein hohes Risiko besteht oder das Rechtsetzungsprojekt den Datenschutz nicht tangiert, kann auf weitere Abklärungen verzichtet werden.

Die Konsultation der Aufsichtsstelle ermöglicht dieser, präventiv und beratend tätig zu werden. Dies ist nicht zuletzt auch für das öffentliche Organ effizienter, da mögliche datenschutzrechtlich problematische Themen bereits in einem frühen Stadium der Datenbearbeitung oder der Rechtsetzung erkannt und behoben werden können.

§ 7b Abs. 2 (neu)

Um neue Projekte besser planen zu können, soll gemäss Abs. 2 den Aufsichtsstellen eine Frist von zwei Monaten zur Erstattung einer Stellungnahme auferlegt werden (ähnlich Art. 28 Richtlinie [EU] 2016/680, Art. 23 DSG). Dies soll nicht zu oberflächlichen Prüfungen führen, weshalb die Frist bei aufwendigen Projekten („bei komplexen Datenbearbeitungen“) um einen Monat erstreckt werden kann.

§ 7b Abs. 3 (neu)

Die Kriterien für die Bearbeitungsvorgänge, die zur Konsultation zu unterbreiten sind, werden bewusst offen gehalten, damit zukünftige Vorgänge und Entwicklungen erfasst werden können.

§ 7c (neu)

Beim Einsatz von künstlicher Intelligenz soll sichergestellt werden, dass auf Verlangen der betroffenen Person ein automatisierter Entscheid zusätzlich durch eine natürliche Person überprüft wird. Zudem soll die betroffene Person über das automatisierte Vorgehen spätestens mit der Einzelentscheidung informiert werden (Art. 11 Richtlinie [EU] 2016/680, Art. 8 Konvention 108+, Art. 21 DSG). Damit wird sichergestellt, dass der Mensch auch in Zukunft über der künstlichen Intelligenz stehen wird.

Das Gesetz sieht nicht vor, dass jede automatisierte Einzelfallentscheidung durch einen Menschen überprüft werden muss. Automatisierte Entscheidungen sollen auch nicht verboten werden, es wird vielmehr festgehalten, dass eine betroffene Person berechtigt

21/31

sein soll, eine automatisierte Entscheidung im Bedarfsfall durch einen Menschen überprüfen zu lassen. Vorbehalten bleiben in Analogie zum Bundesrecht Vollstreckungsentscheide gemäss § 13 Abs. 1 VRG.

Die künstliche Intelligenz ist stets abhängig von der eigenen Programmierung und vom antrainierten oder selbst beschafften Datenbestand. Die daraus resultierenden Entscheide können von den gesetzlichen Vorgaben oder vom gesunden Menschenverstand abweichen. Es ist deshalb wichtig, dass automatisierte Einzelfallentscheide gekennzeichnet werden und die betroffenen Personen die Möglichkeit haben, die Entscheide auf Verlangen von einer natürlichen Person überprüfen zu lassen (Art. 11 Richtlinie [EU] 2016/680, Art. 8 Konvention 108+, Art. 21 DSGVO).

§ 8 Abs. 1 Ziff. 1 (geändert)

Es handelt sich um eine Anpassung des Gesetzestextes zum besseren Verständnis („hierzu“ wird durch „dazu“ ersetzt). Eine inhaltliche Änderung wird nicht vorgenommen.

§ 8 Abs. 1 Ziff. 3 (geändert)

§ 8 Abs. 1 Ziff. 3 sieht vor, dass Einwilligungen nur gültig sind, wenn diese freiwillig und nach angemessener Informationserteilung erklärt wurden (Art. 5 Abs. 2 Konvention 108+, ebenso nicht direkt verpflichtender Art. 7 EU-DSGVO). Die betroffene Person drückt damit ihre Zustimmung zu einer Verletzung der eigenen Persönlichkeit aus, die durch eine nicht durch das Legalitätsprinzip erlaubte Datenbearbeitung erfolgt. Damit die Einwilligung gültig ist, muss die Bearbeitung – wie bereits nach geltendem Recht – insbesondere hinsichtlich Umfang und Zweck hinreichend genau bestimmt sein. Eine eindeutige Einwilligung nach § 8 Abs. 1 Ziff. 3 kann auch durch eine stillschweigende Willenserklärung erfolgen (vgl. Art. 1 Abs. 2 des Obligationenrechts [OR; SR 220]). Eine solche liegt vor, wenn sich die Willensäusserung nicht aus der Erklärung selbst ergibt, sondern durch ein Verhalten, das aufgrund der Umstände, in denen es erfolgt, als eindeutiger Ausdruck des Willens verstanden werden kann (Botschaft DSG, BBl 2017 7027).

Eine Willenserklärung ist „ausdrücklich“, wenn sie durch geschriebene oder gesprochene Worte oder ein Zeichen erfolgt und der geäusserte Willen aus den verwendeten Worten oder dem Zeichen unmittelbar hervorgeht (BGE 121 III 31 E. 2c S. 34, Botschaft DSG, BBl 2017 7028). Dies ist beispielsweise durch das Ankreuzen eines Kästchens, die aktive Auswahl bestimmter technischer Parameter für die Dienste eines Informationsverarbeitungsunternehmens oder anderweitige Erklärungen möglich. Die Einwilligung erfolgt freiwillig, wenn sowohl die Folgen der Einwilligung als auch der Nichteinwilligung bekannt sind und kein sachfremder, unzulässiger Zwang auf die betroffene Person ausgeübt wird (vgl. Botschaft DSG, BBl 2003 2127).

22/31

Auf das Erfordernis der EU-DSGVO, wonach bei Einwilligungen zusätzlich noch das Widerrufsrecht erwähnt sein muss und dabei die Adresse der Widerrufsempfängerin oder des Widerrufsempfängers bekannt zu geben ist, wird aus Praktikabilitätsgründen verzichtet. Die Vorgaben der EU-DSGVO sind nicht schengenrelevant und müssen deshalb nicht übernommen werden.

§ 9 Abs. 1 Ziff. 1 (geändert)

Redaktionelle Anpassung („hierzu“ wird durch „dazu“ ersetzt).

§ 9 Abs. 1 Ziff. 2 (geändert)

Siehe obigen Kommentar zu § 8 Abs. 1 Ziff. 3.

§ 9a Abs. 1 (geändert)

Redaktionelle Anpassung („welche“ wird durch „die“ ersetzt).

§ 9a Abs. 2 (geändert)

Die Zustimmung zur Bearbeitung personenbezogener Daten soll auch im grenzüberschreitenden Datenverkehr nur nach erfolgter angemessener Informationserteilung und ausdrücklich möglich sein (vgl. § 8 Abs. 1 Ziff. 3). Die Möglichkeit einer konkludenten Zustimmung ist nicht vorgesehen.

§ 9a Abs. 3 (neu)

Veröffentlichungen, die gestützt auf das ÖffG erfolgen und im Ausland empfangen werden können, sollen nicht den Einschränkungen zum grenzüberschreitenden Datenverkehr unterliegen (Art. 35 Richtlinie [EU] 2016/680, Art. 14 Konvention 108+, Art. 16 DSGVO).

§ 11 Abs. 1 (geändert)

Redaktionelle Anpassung („Betroffene“ wird durch „betroffenen Personen“ ersetzt).

§ 11 Abs. 1^{bis} (neu)

Die öffentlichen Organe verfügen über viele Daten, die mit Steuergeldern erfasst wurden. Soweit diese Daten bekanntgegeben werden dürfen, soll dies in Form von OGD erfolgen. Dadurch soll erreicht werden, dass diese Daten durch Applikationen Dritter weiterbearbeitet und dadurch der Allgemeinheit in einer anderen Form wieder zur Verfügung gestellt werden können. Die Weitergabe durch das öffentliche Organ hat deshalb, soweit gesetzlich erlaubt, kostenlos und in maschinenlesbarer Form zu erfolgen, damit

23/31

es nicht nur den öffentlichen Organen, sondern auch allen interessierten Privatpersonen ermöglicht wird, entsprechende Applikationen zu erstellen und darin die Daten frei weiterzuverwenden.

Durch die in § 11 Abs. 1^{bis} Satz 3 erfolgte Legitimation des Regierungsrates, ergänzende Vorgaben zum Einsatz von OGD zu erlassen, wird die Möglichkeit geschaffen, Details zu OGD in einer OGD-Verordnung zu regeln. Der Regierungsrat hat dies mit Erlass der am 1. Juni 2025 in Kraft getretenen Open Government Data Verordnung (OGDV; RB 170.72) getan.

§ 12 (Titel geändert)

Zur besseren Verständlichkeit wurde der Titel „Bearbeitung durch Dritte“ in „Bearbeitung im Auftrag“ geändert.

§ 12 Abs. 1 (geändert)

Bisher wurde die Bearbeitung von Personendaten durch Dritte im TG DSG nicht explizit geregelt. Neu soll die bisherige Praxis, bei der Behörden eine Auftragsdatenbearbeiterin oder einen Auftragsdatenbearbeiter beiziehen, durch die Umsetzung von Art. 22 Richtlinie (EU) 2016/680 sowie Art. 9 DSG gesetzlich verankert werden. Das sogenannte „Outsourcing“ ist in der Praxis von grosser Wichtigkeit, da z.B. bereits das Speichern von Daten auf einem Clouddienst als Datenbearbeitung gilt. Falls dafür Daten ins Ausland bekanntgegeben werden, müssen zudem die Voraussetzungen von § 9a eingehalten werden.

Die Bearbeitung von Personendaten kann vertraglich oder durch Gesetz einer Auftragsdatenbearbeiterin oder einem Auftragsdatenbearbeiter übertragen werden, sofern die Daten in gleicher Weise bearbeitet werden, wie es dem verantwortlichen öffentlichen Organ selbst erlaubt wäre, und keine gesetzlichen oder vertraglichen Geheimhaltungspflichten der Übertragung entgegenstehen.

Das öffentliche Organ kann das Bearbeiten von Informationen einer Auftragsdatenbearbeiterin oder einem Auftragsdatenbearbeiter übertragen. Ziff. 1 bis Ziff. 4 nennen die Voraussetzungen, die dafür kumulativ vorliegen müssen:

- Ziff. 1: Es darf keine rechtliche Bestimmung und keine vertragliche Vereinbarung entgegenstehen.
- Ziff. 2: Die Vertraulichkeit muss gewahrt werden. Dies stellt sicher, dass Daten nur von Personen eingesehen, bearbeitet und verwaltet werden, die dazu befugt sind. Das bedeutet, dass das öffentliche Organ gegebenenfalls um Schutzmassnahmen besorgt sein muss (z.B. Verschlüsselung, wobei das Schlüsselmanagement beim Organ bleiben muss).

- Ziff. 3: Es muss sichergestellt sein, dass die beauftragten Dritten Personendaten nur so bearbeiten dürfen, wie es das öffentliche Organ auch tun dürfte. Das betrifft insbesondere die Einhaltung der allgemeinen Grundsätze, die Regeln zur Datensicherheit sowie diejenigen zur Bekanntgabe ins Ausland. Das öffentliche Organ muss Verstösse gegen die Datenschutzgesetzgebung verhindern. Infolgedessen ist es verpflichtet, die beauftragten Dritten sorgfältig auszuwählen, sie angemessen zu instruieren und – soweit als möglich – zu überwachen. Dies geschieht auch im eigenen Interesse des öffentlichen Organs, es bleibt nämlich für den Umgang mit den Informationen auch nach der Übertragung verantwortlich. Ziff. 3 definiert damit eine Sorgfaltspflicht für das verantwortliche Organ.
- Ziff. 4: Die Daten müssen zudem periodisch in einem strukturierten und gängigen Format zurückgegeben werden (Datenportabilität). Mit der Datenportabilität wird gewährleistet, dass Daten beispielsweise im Falle eines Konkurses der Auftragsdatenbearbeiterin oder des Auftragsdatenbearbeiters oder bei einer Unterbrechung der Leitung zur Auftragsdatenbearbeiterin oder zum Auftragsdatenbearbeiter zur Verfügung stehen. In der Praxis hat sich gezeigt, dass es sinnvoll ist, wenn die Behörden die Daten, die ausgelagert sind, wiederherstellen können. Soweit sich jedoch die Daten gleichzeitig auch beim öffentlichen Organ befinden und von diesem gesichert werden können, kann die Anforderung an regelmässige Lieferungen in einem strukturierten Format bereits erfüllt sein. Nur wenn sich die Daten nicht mehr bei den Behörden befinden und diese auf entsprechende Lieferungen für den Notfall angewiesen sind, soll die Regelung gelten.

§ 13 (Titel geändert)

Der überholte Titel „Datensicherung“ wird durch „Informationssicherheit“ ersetzt.

§ 13 Abs. 1 (geändert)

Die Bestimmung zur Datensicherheit wird präzisiert. Die Datenbearbeitung soll neu durch technische und organisatorische Massnahmen vor Verlust, unbefugter Bearbeitung oder unbefugter Kenntnisnahme geschützt werden. Hier handelt es sich um die Regelungen zu technischen Gefahren, was bereits aus dem Titel „Informationssicherheit“ ersichtlich ist (Art. 4, Art. 25 und Art. 29 Richtlinie [EU] 2016/680, Art. 7 Konvention 108+, Art. 8 DSG).

Mit den technischen und organisatorischen Massnahmen sorgt das öffentliche Organ für den Schutz der Personendaten bezüglich ihrer Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit.

§ 13 Abs. 2 (neu)

§ 13 Abs. 2 regelt die Datensicherheit im engeren Sinne. Die Schutzziele (Ziff. 1 bis Ziff. 5) werden im TG DSG normiert, da im Kanton Thurgau kein Informationssicherheitsgesetz existiert.

Typische Massnahmen zur Erreichung angemessener Datensicherheit sind Zugriffsbeschränkungen oder Zugangsbeschränkungen, aber auch Weisungen, Schulungen oder die sorgfältige Auswahl der beauftragten Dritten. Die Massnahmen müssen keinen absoluten Schutz bieten, sondern bei objektiver Betrachtung in einem vernünftigen Verhältnis zum Risiko einer Verletzung der Datensicherheit stehen. Es ist Aufgabe der verantwortlichen Behörde, die notwendigen Massnahmen zu bestimmen.

§ 13 Abs. 2 Ziff. 5 (geändert)

Die Nachvollziehbarkeit von Veränderungen an besonders schützenswerten Personendaten stellt ein zentrales Prinzip der Informationssicherheit dar. Mit der Bestimmung wird gewährleistet, dass die getätigten Datenbearbeitungen bei Einsichtsgesuchen, Kontrollen oder bei Cyberangriffen nachvollziehbar und beweisbar bleiben. Die besonders schützenswerten Personendaten unterliegen einem hohen Schutzbedarf. Jede Änderung dieser Daten kann erhebliche Auswirkungen auf den Schutz der Persönlichkeit der betroffenen Personen haben. Ohne entsprechende Vorgaben zur Nachvollziehbarkeit können unberechtigte Zugriffe oder vorsätzliche Datenmanipulationen weder erkannt noch zurückverfolgt werden. Mit den neu verlangten Änderungsdokumentationen wird die Rechenschaftspflicht über vorgenommene Datenbearbeitungen eingehalten. Unter Berücksichtigung der Verhältnismässigkeit kann bei weniger sensiblen Daten auf eine aufwendige Protokollierung verzichtet werden. Dies verhindert unnötige Bürokratie und fördert eine ressourcenschonende und praktikable Umsetzung der Sicherheitsanforderungen.

§ 13b Abs. 1 (neu)

Es wird eine Informationspflicht der betroffenen Person eingeführt, damit diese über die Beschaffung von Personendaten informiert wird (Art. 13 und Art. 14 Richtlinie [EU] 2016/680, Art. 8 Konvention 108+, Art. 19 DSG). Die Information hat angemessen, beispielsweise durch die Information im Register der Datensammlungen, auf der Internetseite des entsprechenden öffentlichen Organs oder durch direkte Mitteilung an die betroffene Person, zu erfolgen. Die Informationspflicht gilt gemäss § 13b Abs. 1 S. 2 auch, wenn die Daten bei Dritten beschafft wurden.

§ 13b Abs. 2 (neu)

Die in § 13b Abs. 2 normierten Mindestangaben sind erforderlich, damit die betroffenen Personen ihre Auskunfts-, Berichtigungs-, Löschungs- oder Widerspruchsrechte geltend machen können. Durch die Bekanntgabe der verantwortlichen Stelle, des Bearbeitungszwecks und allfälliger Datenempfänger und -empfängerinnen wird die nötige Transparenz geschaffen, die als Grundlage für das Vertrauen der Bevölkerung in den Umgang der öffentlichen Organe mit Personendaten dient. In einem demokratischen Rechtsstaat ist es wichtig, dass jedes staatliche Handeln, und dazu gehört auch die Datenbearbeitung durch öffentliche Organe, nachvollziehbar und überprüfbar ist. Deshalb wird neu eine aktive Information über das Beschaffen von Personendaten verlangt, die in Einklang mit den Vorgaben des übrigen Rechts steht (Art. 13 Richtlinie [EU] 2016/680, Art. 8 Konvention 108+, Art. 19 DSGVO).

§ 13b Abs. 3 (neu)

Die Informationspflicht entfällt, wenn die betroffene Person bereits über die Information nach Abs. 2 verfügt (Ziff. 1), das Bearbeiten der Personendaten gesetzlich ausdrücklich vorgesehen ist (Ziff. 2), die Erfüllung einer gesetzlichen Aufgabe des verantwortlichen Organs verunmöglicht wird (Ziff. 3) oder die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist (Ziff. 4). Da sich die öffentlichen Organe bereits für die Bearbeitung von Personendaten auf eine gesetzliche Grundlage abstützen müssen, wird die Informationspflicht nur ausnahmsweise Anwendung finden und somit zu keinem nennenswerten Aufwand führen.

§ 13c

Beim Einsatz von IT-Systemen besteht ein gewisses Restrisiko. Damit die Folgen allfälliger Datenschutzverletzungen minimiert werden können, sind Datenschutzverletzungen umgehend zu melden. Aufgrund der Meldung kann anschliessend beurteilt werden, ob und gegebenenfalls welche weiteren Massnahmen zielführend ergriffen werden müssen (Art. 30 f. Richtlinie [EU] 2016/680, Art. 7 Konvention 108+, Art. 24 DSGVO). Da heute noch nicht absehbar ist, wie viele und welche Verletzungen eintreffen werden, können die möglichen Risiken und Massnahmen nicht abschliessend aufgeführt werden.

§ 17 Abs. 1^{bis} (neu)

§ 17 Abs. 1^{bis} legt fest, dass der oder die vom Regierungsrat gewählte Datenschutz- und Öffentlichkeitsbeauftragte fachlich geeignet sein muss (z.B. Qualifikation, Fachkenntnis und Erfahrung im Bereich des Datenschutzes). Die Verankerung von § 17 Abs. 1^{bis} im TG DSGVO ist eine Vorgabe aus übergeordnetem Recht (EU Art. 43 Abs. 2 Richtlinie 2016/680).

27/31

§ 17 Abs. 2 (geändert)

Redaktionelle Anpassung („Dieser“ wird durch „Diese Person“ ersetzt).

§ 17 Abs. 3 Satz 2 (geändert)

Unverändert bleibt, dass die Gemeinden eigene Datenschutzstellen bezeichnen. Da dies teilweise zu Interessenkollisionen führte, wurde durch Abs. 3 Satz 2 die Möglichkeit der Stellvertretung durch Aufsichtsstellen anderer Gemeinden geschaffen.

Im Vernehmlassungsverfahren wurde angeregt, dass nicht nur andere Gemeinden, sondern auch eine andere externe Stelle (z.B. eine Anwältin oder ein Anwalt) die Stellvertretungsfunktion übernehmen könnte. Zudem wurde beantragt, das Wort „drohende“ in „potentielle“ zu ändern. Diese Vorschläge sind zu begrüßen. Der Gesetzestext wurde entsprechend angepasst.

§ 18 Abs. 1 (geändert)

Der Umfang der Beratung wurde der Regelung in § 6 ÖffG angepasst. Er richtet sich nach den internationalen Vorgaben (Art. 46 Richtlinie [EU] 2016/680).

§ 18 Abs. 4 (geändert)

Redaktionelle Anpassung („ihn“ wird durch „den Regierungsrat“ ersetzt).

§ 18b (neu)

In der Botschaft DSG wird festgehalten, dass die Stellung des oder der Datenschutz- und Öffentlichkeitsbeauftragten gemäss den internationalrechtlichen Vorgaben zwingend gestärkt werden muss (vgl. BBl 2017 6943 f., Art. 47 Richtlinie [EU] 2016/680, Art. 12 Konvention 108+, Art. 51 DSG).

§ 18b Abs. 1 bis 5 (neu)

Bisher konnte der oder die Datenschutz- und Öffentlichkeitsbeauftragte im Bereich des Datenschutzes lediglich Empfehlungen abgeben. Neu soll der oder die Datenschutz- und Öffentlichkeitsbeauftragte auch Entscheide fällen dürfen (§ 18b Abs. 3). Die Verfügung könnte beispielsweise darauf lauten, eine widerrechtliche Datenbearbeitung einzustellen oder auf eine widerrechtliche Datenbearbeitung zu verzichten. Dieses Instrument wird der Aufsichtsstelle allerdings nur im Sinne einer „ultima ratio“ offenstehen, wenn ein öffentliches Organ einer Empfehlung nicht Folge leistet oder klar zu erkennen gibt, dass es dies nicht tun wird.

28/31

Zudem soll der oder die Datenschutz- und Öffentlichkeitsbeauftragte vorsorgliche Massnahmen treffen können (§ 18b Abs. 5). Dies gilt gemäss der Botschaft DSG nicht nur für den EDÖB, sondern auch für die entsprechenden Funktionärinnen und Funktionäre auf Kantonsebene (vgl. Botschaft DSG, BBl 2017 7180). Aus diesem Grunde ist zwingend auch eine dem Art. 51 DSG entsprechende Regelung im TG DSG aufzunehmen.

5. Rechte der betroffenen Person (Titel geändert)

Der Titel von Abschnitt 5 wird von „Rechte der Betroffenen“ in „Rechte der betroffenen Person“ geändert.

§ 20 Abs. 1 (geändert)

Redaktionelle Anpassung („Jedermann“ wird durch „Jede Person“ und „über ihn“ wird durch „über sie“ ersetzt).

§ 20a (aufgehoben)

§ 20a wird aufgehoben und in § 23c neu gefasst.

§ 21 Abs. 2 (aufgehoben)

Die Bestimmung wird aufgehoben.

§ 22 Abs. 1 (geändert)

Gesuche um Berichtigung falscher Personendaten sollen neu wie die Einsichtnahme in die eigenen Daten kostenlos sein und zudem innert angemessener Frist erledigt werden (Art. 46 Abs. 3 Richtlinie [EU] 2016/680, Art. 32 und Art. 59 DSG).

§ 22 Abs. 3 (geändert)

Sofern weder die Richtigkeit noch die Unrichtigkeit von Personendaten bewiesen werden kann, muss das öffentliche Organ darauf hinweisen, dass die betreffende Person mit dem Dateninhalt nicht einverstanden ist. Das öffentliche Organ muss diese Personendaten mit einem Bestreitungsvermerk versehen.

§ 23 Abs. 1 (geändert)

Redaktionelle Anpassung („ein Betroffener“ wird durch „eine betroffene Person“ ersetzt).

29/31

§ 23b (neu)

Nach bisherigem Recht stand der betroffenen Person lediglich der Rechtsmittelweg zur Verfügung, wenn ein öffentliches Organ die Ansprüche bezüglich beanstandeter Datenbearbeitung nicht anerkannte. Neu sollen bei dem oder der Datenschutz- und Öffentlichkeitsbeauftragten aufsichtsrechtliche Anzeigen eingereicht werden können. Dieser oder diese hat der anzeigenden Person spätestens innert drei Monaten Auskunft über das Ergebnis der Abklärungen zu erstatten (Art. 17 und Art. 52 Richtlinie [EU] 2016/680, Art. 49 DSGVO).

Die in § 74 und § 75 VRG geregelte Anzeige unterscheidet sich von der aufsichtsrechtlichen Anzeige nach § 23b. Während im Rahmen des VRG jedermann der Aufsichtsbehörde (vermeidliche) Missstände zur Kenntnis bringen kann, geht es in § 23b um eine konkret betroffene Person, die betreffend ihrer eigener Personendaten Anzeige erstattet.

5a. Gebühren und Rechtsmittel (neuer Abschnitt)

Im Sinne einer besseren Gliederung des Gesetzes wird ein neuer Abschnitt 5a geschaffen. Die Bestimmungen über Unentgeltlichkeit und Gebühren (§ 23c) sowie Rechtsmittel (§ 24) werden in diesen Abschnitt verschoben.

§ 23c Abs. 1 (neu)

Entsprechend der bisherigen gesetzlichen Regelung soll die Einsichtnahme in die eigenen Daten und die Auskunftserteilung über eigene Daten kostenlos erfolgen. Das Recht auf Auskunft ist einer der wichtigsten Ausflüsse des Grundrechts auf Datenschutz, weshalb dessen Geltendmachung und die sich aus dem Recht der Auskunftserteilung ergebenden weiteren Rechte der betroffenen Person nicht durch Gebührenerhebung erschwert werden soll.

§ 23c Abs. 2 (neu)

Diese Bestimmung sieht eine Ausnahme von der Unentgeltlichkeit gemäss Abs. 1 vor. In Analogie zu Art. 2 der Verordnung zum Bundesgesetz über den Datenschutz in der bis zum 1. September 2023 geltenden Fassung (aVD SG; SR 235.11) soll die mehrfache Einsicht und Auskunft in die eigenen, unveränderten Daten bei mehreren Gesuchen innerhalb eines Jahres nicht mehr kostenlos sein (Art. 46 Abs. 4 Richtlinie [EU] 2016/680, ähnlich Art. 21 Konvention 108+). Der Grundsatz der Kostenlosigkeit darf nur unter klar definierten Voraussetzungen aufgehoben werden.

§ 23c Abs. 3 (neu)

Anders verhält es sich bei Rechtsberatungen. Der oder die Datenschutz- und Öffentlichkeitsbeauftragte soll keine Konkurrenz zu privatrechtlichen Rechtsberatungen darstellen. Dies ergibt sich auch aus Art. 46 der Richtlinie (EU) 216/680. Dort wird einzig festgehalten, dass die Kostenlosigkeit nur für die in der Richtlinie genannten Aufgaben der Aufsichtsbehörden besteht. Die Rechtsberatung gehört nicht zu den in Art. 47 der Richtlinie (EU) 216/680 genannten Aufgaben, weshalb in diesem Bereich die grundsätzliche Kostenlosigkeit aufgehoben werden kann.

Im DSG besteht für die Schulung und Beratung von Privaten eine Kostenpflicht. Entsprechend soll nun auch im Kanton Thurgau eine gesetzliche Grundlage geschaffen werden, mit der Schulungen und Beratungen von privaten Personen kostenpflichtig erklärt werden können (analog Art. 59 DSG).

6. Strafbestimmungen (Titel Gliederung geändert)

Der Titel des 6. Abschnitts wird von „Straf- und Schlussbestimmungen“ in „Strafbestimmungen“ geändert.

§ 25 und 26 (aufgehoben)

Diese Bestimmungen sind obsolet und können gestrichen werden.

5. Gesetz über das Einwohnerregister sowie kantonale Register (ErG)

Das Gesetz über das Einwohnerregister sowie kantonale Register (ErG; RB 142.15) wird in § 13c mit einem neuen Abs. 5 ergänzt. Mit dieser Ergänzung soll festgehalten werden, dass das Amt für Geoinformation (AGI) Zugriff auf die Personen- und Sachregisterdaten erhält und diese in einem eigenen Datenbestand speichern darf. Davon ausgenommen sind besonders schützenswerte Personendaten. Mit dieser neuen Regelung soll erreicht werden, dass die Daten vom AGI an hoheitlich tätige Dritte weitergegeben werden dürfen, soweit dies gesetzlich erlaubt ist. Selbstverständlich werden dadurch die übrigen Anforderungen, z.B. dass der Regierungsrat auch den Zugriff durch die jeweiligen Dritten zu regeln hat, nicht aufgehoben. Bei der Aufnahme von weiteren zugriffsberechtigten Dritten ist deshalb auch in Zukunft immer ein neues Gesuch zu stellen.

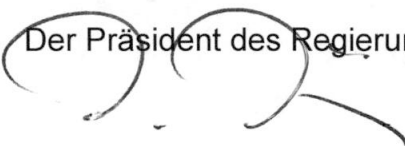
6. Inkrafttreten

Die Änderungen treten auf einen durch den Regierungsrat zu bestimmenden Zeitpunkt in Kraft.

31/31

7. Antrag

Wir ersuchen Sie, sehr geehrter Herr Präsident, sehr geehrte Damen und Herren, den Gesetzesentwurf Ihrer Beratung zu unterziehen und uns über die Beschlüsse in üblicher Weise zu benachrichtigen.


Der Präsident des Regierungsrates

Der Staatsschreiber





Beilagen:

- Entwurf des Regierungsrates
- Synopse