Hinweise des Thüringer Innenministeriums zum
Thüringer Datenschutzgesetz - ThürDSG -

vom 07. Februar 2003

Allgemeines:

Ziel des Datenschutzes ist es, den Einzelnen beim Umgang mit seinen Daten in seinem Persönlichkeitsrecht, seiner Privatsphäre vor unzulässiger Beeinträchtigung zu schützen. Nachfolgende Ausführungen zum in der Bekanntmachung vom 10.10.2001 (GVBl. S. 276) vorliegenden ThürDSG haben erläuternden und kommentierenden Charakter. Sie sollen dem vom Anwendungsbereich des ThürDSG erfassten Nutzer als Arbeitshilfe ergänzend zu anderen datenschutzrechlichen Regelungen dienen und spezielle datenschutzrechliche Grundsätze verdeutlichen.

Das novellierte ThürDSG setzt die Maßgaben 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. Nr. EG L 281 S. 31) – EG-Datenschutzrichtlinie – in dem erforderlichen Umfang um.

Thüringen hat von der im Bundesdatenschutzgesetz (BDSG) in § 1 Abs. 2 i.V.m. § 12 Abs. 2 enthaltenen Option umfassend Gebrauch gemacht und den Datenschutz für die öffentlichen Stellen des Landes im Thüringer Datenschutzgesetz (ThürDSG) abschließend geregelt. Soweit daher das ThürDSG selbst nichts anderes bestimmt (vgl. z. B. in § 26), finden die Vorschriften des BDSG auf öffentliche Stellen des Landes keine Anwendung. Eine Ausnahme ergibt sich aus § 81 Abs. 4 des Zehnten Buches zum Sozialgesetzbuch (SGB X): Soweit Thüringer Sozialversicherungsträger (Kranken-, Renten- und Unfallversicherungsträger) das SGB vollziehen, gelten für diese ergänzend zu den materiell-rechtlichen Vorschriften über den Schutz von Sozialdaten auch die formalrechtlichen Vorschriften des BDSG bezüglich der Bestellung behördeninterner Datenschutzbeauftragter und der Führung des Verfahrensverzeichnisses.

Der Geltungsbereich des BDSG erstreckt sich auf den Datenschutz für die öffentliche Verwaltung des Bundes sowie für die Datenverarbeitung und Nutzung bei nicht öffentlichen Stellen.

Das ThürDSG räumt den Betroffenen Schutzrechte ein, die sie gegenüber den Daten verarbeitenden Stellen geltend machen können. Zur Kontrolle der Einhaltung der Vorschriften des Datenschutzes werden vom Gesetz wirksame Kontrollinstanzen geschaffen.

Das ThürDSG ist - wie das BDSG - ein Auffanggesetz. Es gilt nur, soweit im Einzelfall keine besonderen Rechtsvorschriften des Bundes oder des Landes auf den Umgang mit personenbezogenen Daten anwendbar sind. Auf den Rang der Rechtsvorschriften kommt es dabei nicht an; es können Gesetze, Verordnungen oder

Zu den Einzelvorschriften des ThürDSG

Zu § 1 ThürDSG

1.1 Im Mittelpunkt des Gesetzes steht das durch Artikel 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 des Grundgesetzes gewährleistete allgemeine Persönlichkeitsrecht natürlicher Personen. Dabei geht es um die Gewährleistung dieses Rechts beim Umgang öffentlicher Stellen mit persönlichen Daten.

1.2 Zum Begriff „personenbezogene Daten“ vgl. Ziff. 3.1.

Zu § 2 ThürDSG

2.1 § 2 Abs. 1 ThürDSG benennt die Adressaten des ThürDSG und erfasst mit der Legaldefinition der öffentlichen Stellen zugleich den gesamten Bereich der öffentlichen Verwaltung des Landes, unabhängig davon, ob Bundes- oder Landesrecht vollzogen wird. Der Begriff der „öffentlichen Stelle“ ist auch maßgeblich für die Festlegung der „Daten verarbeitenden Stelle“.

Soweit Absatz 1 den Begriff „Behörde“ i.S. § 1 Abs. 2 Thüringer Verwaltungsverfahrensgesetz (ThürVwVfG) verwendet, stellt das Gesetz auf den organisatorischen (nicht auf den funktionalen) Behördenbegriff ab. Maßgeblicher Anknüpfungspunkt ist demzufolge die nach außen hin bestehende Aufbauorganisation, nicht dagegen die konkret wahrgenommene Aufgabe (Funktion). Äußeres Zeichen der organisatorischen Selbstständigkeit ist insbesondere die Befugnis zum eigenverantwortlichen Auftreten im eigenen Namen nach außen.

Außer für Behörden und Gerichte gilt das Gesetz auch für die sonstigen öffentlichen Stellen des Landes, der Gemeinden und Gemeindeverbände.

Sonstige öffentliche Stellen sind nach außen hin eigenverantwortlich handelnde Stellen, die keine Behördeneigenschaft besitzen, z. B. die Gerichte als Spruchkörper, der Landtag als Parlament, Stellen mit lediglich fiskalischen Aufgaben. Soweit öffentliche Stellen am Wettbewerb teilnehmen, bestimmt sich die Anwendung nach § 26 ThürDSG.

2.2 § 2 Abs. 2 ThürDSG klärt die Frage, in welchen Fällen das Gesetz auch auf Vereinigungen des privaten Rechts wie Kapitalgesellschaften, Personengesellschaften sowie rechtsfähige und nicht rechtsfähige Vereine anzuwenden ist.

Vereinigungen, an denen ausschließlich öffentliche Stellen beteiligt sind, gelten auch dann als öffentliche Stellen, wenn sie nicht öffentlich-rechtlich organisiert sind (z.B., wenn die Form einer GmbH gewählt wird).

Für Vereinigungen des privaten Rechts, an denen neben den in Absatz 1 genannten juristischen Personen des öffentlichen Rechts auch nicht öffentliche Stellen beteiligt sind, ist im Hinblick auf die Geltung als öffentliche Stelle i.S. des ThürDSG maßgeblich, dass sie Aufgaben der öffentlichen Verwaltung wahrnehmen. Voraussetzung hierfür ist außerdem, dass Identität zwischen den von der Vereinigung wahrgenommenen Aufgaben der öffentlichen Verwaltung und den Aufgaben der konkret beteiligten juristischen Person des öffentlichen Rechts besteht.

Als Aufgaben der öffentlichen Verwaltung kommen hierbei beispielsweise die Energie- und Wasserversorgung sowie die Gewährleistung des örtlichen öffentlichen Personennahverkehrs als Aufgaben des eigenen Wirkungskreises der Gemeinden nach § 2 Abs. 2 Thüringer Kommunalordnung (ThürKO) und die Krankenhausversorgung durch das Land, die Landkreise und kreisfreien Städte nach § 2 Thüringer Krankenhausgesetz in Betracht. Nicht ausreichend sind Aufgaben, die lediglich im öffentlichen Interesse liegen.

Der Begriff der Vereinigung ist auch erfüllt, wenn eine Gesellschaft nur aus einem Gesellschafter besteht, auf den die Kriterien einer öffentlichen Stelle zutreffen.

Bei den nicht öffentlichen Stellen, die hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen, handelt es sich um sogenannte „beliehene Unternehmer". Beliehene Unternehmer sind Privatrechtssubjekte (wie z. B. Kfz-Sachverständige des TÜV und öffentlich bestellte Vermessungsingenieure), denen bestimmte Aufgaben und Befugnisse der öffentlichen Verwaltung im Wege der Delegation durch oder aufgrund Rechtsnorm zugewiesen sind.

2.3 Bezüglich der in Absatz 3 enthaltenen Vorrangregelung vgl. Ausführungen in der Einleitung unter Allgemeines.

2.4 § 2 Abs. 4 ThürDSG stellt klar, dass auch bei der Ermittlung eines Sachverhalts im Verwaltungsverfahren die Vorschriften des ThürDSG gegenüber den Vorschriften des ThürVwVfG vorrangig sind. Dies bezieht sich insbesondere auf den Untersuchungsgrundsatz (§ 24 ThürVwVfG) und auf die Beweismittel, die eine Behörde im Verwaltungsverfahren beiziehen kann (§ 26 ThürVwVfG). Eine um Amtshilfe ersuchte Stelle darf bei der Verarbeitung und Nutzung personenbezogener Daten Amtshilfe nur leisten, soweit dies nach den Vorschriften des ThürDSG zulässig ist (§ 5 Abs. 2 Nr. 1 ThürVwVfG).

2.5 Gerichte werden in Verwaltungsangelegenheiten tätig, wenn sie Aufgaben erfüllen, die weder im unmittelbaren noch im mittelbaren sachlichen oder organisatorischen Zusammenhang mit der Verwirklichung unmittelbaren Rechtsschutzes im Einzelfall, d.h. mit der Rechtsprechung oder sonstiger Formen der individuellen Rechtspflege (z. B. freiwillige Gerichtsbarkeit) stehen. Allgemein sind Verwaltungsangelegenheiten solche Angelegenheiten, die Gegenstand eines Rechtsstreits gemäß § 23 EGGVG sein können. Darüber hinaus betrifft dies Angelegenheiten der Personal- und Gebäudeverwaltung, Beschaffung und Verwaltung von Sachmitteln, Führung von Adress- und Telefonverzeichnissen einschließlich der für die Durchführung dieser Tätigkeiten erforderlichen Hilfstätigkeiten (z. B. Schreibdienst, Aktentransport). Verwaltungsangelegenheiten sind ferner Ausübung der Dienstaufsicht (auch über Richter), Gewährung von Akteneinsicht in bzw. Auskunfterteilung aus Gerichtsakten nach Abschluss eines Verfahrens, Justizmitteilungen, Verwaltung der Akten über abgeschlossene Verfahren, Aufsicht über Notare. Im Übrigen gilt für Gerichte das unter Ziff. 2.3 Ausgeführte.

Zu § 3 ThürDSG

3.1 Der Begriff Einzelangaben über persönliche oder sachliche Verhältnisse einer natürlichen Person (Betroffener) ist weit zu fassen. Darunter fallen nicht nur Daten, an deren Geheimhaltung der Betroffene ein Interesse hat (Geheimnisse), sondern auch jedwede sonstige Angabe zur Person. Beispiel: Name, Vorname, Wohnort, Geburtsdatum, Telefonnummer, Haarfarbe etc. Einzelangaben sind aber auch Daten, die weitere, in der Person des Betroffenen liegende oder auf den Betroffenen bezogene Sachverhalte beschreiben (z. B. Einkommen, Familienstand, Staatsangehörigkeit, Krankheiten, Zeugnisnoten, Berufsbezeichnung, Religionszugehörigkeit, Eigentümer- und Haltereigenschaften); auch Werturteile sowie Planungs- und Prognosedaten gehören dazu, soweit sie einer natürlichen Person konkret zugeordnet werden können. Nicht personenbezogen sind Daten über juristische Personen (sowohl des privaten als auch des öffentlichen Rechts) oder Personenvereinigungen (z. B. offene Handelsgesellschaften, nicht rechtsfähige Vereine), soweit kein Rückschluss auf natürliche Personen möglich ist. Bestimmt ist eine Person, wenn ihre Identität unmittelbar aus den vorliegenden Unterlagen feststellbar ist. Im Regelfall ist hierfür der Name und bei Namensgleichheiten ein weiteres Merkmal erforderlich, aber auch ausreichend. Bestimmbar ist eine Person, wenn ihre Identität mit Hilfe anderer verfügbarer Daten (Zusatzwissen) oder durch besondere äußere Umstände hergestellt werden kann (z. B. Kfz.-Kennzeichen). Nicht bestimmbar ist eine Person, wenn ihre Daten mit Daten anderer Personen zusammengefasst (aggregiert), anonymisiert (vgl. § 3 Abs. 9 ThürDSG) oder pseudonymisiert (vgl. § 3 Abs. 10 ThürDSG) sind, soweit die Zuordnungsfunktion nicht bekannt ist.

Nicht zu den natürlichen Personen gehören Verstorbene. Ihre Rechte werden nicht nach dem ThürDSG geschützt. Jedoch können hier andere Vorschriften sowie Strafnormen greifen, die den Schutz des Andenkens Verstorbener regeln, oder Archivvorschriften zu beachten sein, die über den Tod hinaus wirken. Informationen über Verstorbene können aber auch Bezüge zu lebenden Personen haben und zum Schutz des Persönlichkeitsrechts dieser Betroffenen dem Datenschutzrecht unterliegen.

3.2 Die Bestimmung in § 3 Abs. 2 ThürDSG folgt dem in Art. 3 Abs. 1 der EG-Datenschutzrichtlinie verwandten Begriff der automatisierten Verarbeitung, wonach es auf die Datenorganisation (die Spannbreite reicht von Datenbanken bis zu unformatiertem Fließtext) in keiner Weise ankommt. Wesentliche Kriterien sind der Ablauf der Verarbeitung durch gesteuerten Einsatz von Technik ohne weiteres menschliches Zutun. Allerdings muss sich die automatisierte Verarbeitung nicht nur auf den Datenträger, sondern auf die Daten mit ihrer inhaltlichen Dimension beziehen. Jede hierdurch entstehende Sammlung personenbezogener Daten, die programmgesteuert ausgewertet werden kann, ist eine automatisierte Datei. Die offene Formulierung erlaubt zugleich, auch künftigen technischen Entwicklungen gerecht zu werden.

3.3 § 3 Abs. 3 ThürDSG benennt die einzelnen Phasen der Datenverarbeitung. Mit Blick auf die Begriffsbestimmung in der EG-Datenschutzrichtlinie umfasst der Begriff der Verarbeitung nunmehr auch die bisher gesondert geregelte Phase der Erhebung.

3.3.1 Unter Erheben fällt jegliche Form der zielgerichteten Informationsgewinnung, ungeachtet der dazu verwendeten Medien, Datenübertragungswege und Datenaufnahmeverfahren. Das Erfassen bereits bei der Daten verarbeitenden Stelle in Aktenform vorhandener Daten auf Karteikarten oder auf Datenträger für automatisierte

Verfahren stellt keine Erhebung i. S. v. § 3 Abs. 3 Nr. 1 ThürDSG dar.

3.3.2 Die Speicherung beginnt beim Erfassen oder Aufnehmen personenbezogener Daten auf einem Datenträger (z. B. auf Magnetplatten, Karteikarten, Akten) zum Zwecke ihrer weiteren Nutzung. Die Speicherung umfasst auch die Aufbewahrung von Daten. Sie endet mit der Löschung der Daten.

3.3.3 Eine Übermittlung von personenbezogenen Daten liegt nicht schon dann vor, wenn die Daten zur Einsichtnahme bereitgehalten werden; die Übermittlung erfolgt vielmehr erst in dem Moment, in dem der Empfänger die Daten einsieht oder abruft. Keine Übermittlungen sind die Weitergabe von Daten an den Betroffenen selbst und die Weitergabe von Daten zwischen Auftraggeber und Auftragnehmer bei Auftragsdatenverarbeitung (vgl. § 3 Abs. 6 ThürDSG).

3.3.4 Eine Sperrung personenbezogener Daten kann für einzelne Daten, für Datensätze oder ganze Datenbestände erfolgen. Gesperrte Daten sind zur Verhinderung einer unbeabsichtigten Verwendung durch geeignete Mittel (Markierungen, Randvermerke u. ä.) als solche zu kennzeichnen.

3.3.5 Löschen ist das endgültige Unkenntlichmachen gespeicherter personenbezogener Daten.

Die Löschung bedarf stets geeigneter technischer Maßnahmen (§ 9 ThürDSG); organisatorische Festlegungen allein reichen nicht. Bei der Löschung von Daten in Akten ist in der Regel die gesamte Unterlage zu vernichten. Die Löschung von Daten auf magnetischen Datenträgern verlangt den Einsatz spezieller Software, mit deren Hilfe die Datenträger vollständig überschrieben werden (Löschkommandos allein bewirken keine vollständige Löschung des Inhalts des jeweiligen Speichermediums). Insbesondere bei Aussonderung und Verkauf ist darauf zu achten, dass die Daten auf den magnetischen Datenträgern auch physisch gelöscht sind, so dass eine Rekonstruktion mit hoher Wahrscheinlichkeit ausgeschlossen ist.

Bei besonders sensiblen Daten sind die Speichermedien im Regelfall mechanisch, thermisch oder magnetisch zu löschen. In den Löschvorgang sind unter Berücksichtigung der Bestimmungen in § 16 Abs. 4 ThürDSG alle Datenträger, auch Datensicherungskopien, einzubeziehen, auf denen die betreffenden Daten vorgehalten werden.

Beauftragen öffentliche Stellen andere Personen oder Stellen mit der Löschung personenbezogener Daten (z. B. Entsorgung von Datenträgern/Aktenvernichtung) sind die Bestimmungen des § 8 ThürDSG zu beachten. Soweit hier der Umgang mit den personenbezogenen Daten besonderen Geheimhaltungsbestimmungen unterliegt (z. B. Arztgeheimnis), ist zu gewährleisten, dass eine Kenntnisnahme der Daten durch den Auftragnehmer unmöglich wird (z. B. durch Beaufsichtigung der Vernichtung oder Vor-Ort-Vernichtung).

3.4 Der Begriff des Nutzens hat die Funktion eines Auffangtatbestandes. So wird sichergestellt, dass der Anwendungsbereich des Gesetzes alle Formen der Verwendung personenbezogener Daten erfasst, das heißt auch solche, die keine Verarbeitung darstellen.

3.5 Der Begriff „Daten verarbeitende Stelle“ ist inhaltlich identisch mit dem der öffentlichen Stelle (vgl. hierzu 2.1) und folgt insofern dem organisatorischen Behördenbegriff. Daten verarbeitende Stelle ist stets eine öffentliche Stelle in ihrer organisatorischen Gesamtheit – z. B. ein Landratsamt einschließlich aller Dezernate und Ämter. Bedeutung kommt dem Begriff für die Beurteilung der Frage zu, ob eine Weitergabe von Daten eine Datenübermittlung an eine andere Daten verarbeitende Stelle oder eine Datennutzung innerhalb ein und derselben Daten verarbeitenden Stelle darstellt.

3.6 Der Begriff des Empfängers ist entsprechend der EG-Datenschutzrichtlinie weiter als der Begriff des Dritten gefasst. Er umfasst jede Person oder Stelle, die Daten über den Betroffenen erhält, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

Empfänger sind alle, die Daten erhalten in ihrer Eigenschaft als

- Dritte,
- Personen oder Stellen, die für die verantwortliche Stelle personenbezogene Daten im Auftrag verarbeiten oder nutzen oder
- ein anderer Organisationsteil der Daten verarbeitenden Stelle, dem Daten für andere Zwecke zur Verfügung gestellt werden.

Betroffene sind nicht Empfänger im Sinne dieses Gesetzes.

Der Begriff des Dritten ist ein wesentliches Element des Begriffs der Übermittlung; insbesondere entscheidet er über die Abgrenzung zwischen der Übermittlung und der Nutzung.

Dritter ist grundsätzlich jede Person oder Stelle außerhalb der Daten verarbeitenden Stelle und damit jede Stelle, die nicht mit der Daten verarbeitenden Stelle identisch oder ein Teil von ihr ist. Maßgebend ist hierbei die juristische, nicht die wirtschaftliche Betrachtungsweise.

Betroffene sowie Stellen, die im Geltungsbereich der EG-Datenschutzrichtlinie personenbezogene Daten im Auftrag verarbeiten oder nutzen, sind keine Dritten.

3.7 Mit der Definition des Dateienbegriffs in § 3 Abs. 7 ThürDSG wird den Maßgaben des Artikel 2 Bst. c) EG-Datenschutzrichtlinie entsprochen. Neben der Notwendigkeit, dass die Sammlung strukturiert sein, d.h. eine äußere Ordnung aufweisen muss, müssen die Daten nach bestimmten Kriterien zugänglich sein. Damit ist gemeint, dass inhaltliche Erschließungsmöglichkeiten bestehen, etwa durch ein der Sammlung zugeordnetes System, das eine programmgesteuerte Suche mit Hilfe von Identifikations- oder Sachmerkmalen erlaubt (automatisierte Datei), oder eine vorhandene alphabetische oder chronologische Sortierung einer Kartei (nicht automatisierte Datei). Die Definition stellt darüber hinaus klar, dass eine Datei auch dann vorliegt, wenn die Auswertungskriterien erst bei der Systemnutzung bestimmt werden. Im Übrigen wird die bisherige Definition beibehalten, weil sie in bereichsspezifischen Rechtsvorschriften zum Datenschutz noch verwendet wird.

3.8 Das ThürDSG beschränkt sich - anders als das BDSG für den nicht öffentlichen Bereich - bei seiner Anwendung nicht auf den Umgang mit personenbezogenen Daten in automatisierten Verfahren und die Verarbeitung von Daten in oder aus nicht-automatisierten Dateien. Daher legt das Gesetz für Akten einzelne differenzierende Regelungen fest, die auf die Besonderheiten dieses Mediums abstellen. Akte ist, abweichend vom allgemeinen Sprachgebrauch, jede sonstige amtlichen, dienstlichen oder Geschäftszwecken dienende Unterlage, die nicht Datei ist. Bild- und Tonträger sind danach Akten, sofern sie nicht bereits als nicht-automatisierte Dateien einzustufen sind oder Teil eines automatisierten Verfahrens sind. Nicht vom Aktenbegriff erfasst werden Notizen und Vorentwürfe. Die Sonderregelungen für Akten und Aktensammlungen gelten nicht, soweit sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können. Das entsprechende Verfahren muss eingerichtet und einsatzbereit sein.

3.9 § 3 Abs. 9 ThürDSG enthält die Definition des Anonymisierens und stellt klar, dass personenbezogene Daten nicht nur dann anonymisiert sind, wenn ein Personenbezug überhaupt nicht mehr herstellbar ist, sondern auch dann, wenn die Zuordnung nur noch mit unverhältnismäßigem Aufwand an Zeit, Kosten und Arbeitskraft möglich wäre (faktische Anonymisierung). Je sensibler die Daten sind, desto größer muss der Aufwand sein, sie zu einer Person wieder zuordnen zu können.

3.10 Pseudonymisieren ist das Verändern personenbezogener Daten durch Verwendung einer Zuordnungsregel derart, dass mit verhältnismäßigem Aufwand Einzelangaben nur in Kenntnis dieser Regel einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. An die Stelle identifizierbarer Daten tritt ein Pseudonym, das es ermöglicht, Daten ohne Kenntnis der Identität des Betroffenen zu nutzen. Bei der Wahl der Zuordnungsfunktionen ist darauf zu achten, dass die Pseudonyme möglichst wenig Informationsgehalt aufweisen. Pseudonyme können unterschiedlich gestaltet sein: Vergabe des Pseudonyms durch die betroffene Person, Vergabe des Pseudonyms durch einen vertrauenswürdigen Dritten, der allein über die Zuordnungsregel verfügt, Vergabe des Pseudonyms durch den Datenverwender.

Zu § 4 ThürDSG

4.1 Andere Rechtsvorschrift im Sinne des § 4 Abs. 1 ThürDSG ist jede Rechtsnorm (Gesetz oder Verordnung oder Satzung).

4.2 Soweit die Verarbeitung personenbezogener Daten nicht durch das ThürDSG selbst oder eine andere Rechtsvorschrift erlaubt oder vorgeschrieben wird, dürfen personenbezogene Daten nur mit Einwilligung des Betroffenen verarbeitet werden.

4.3 Einwilligung ist die vorherige, freiwillige Zustimmung des Betroffenen. Sie ist schriftlich zu erteilen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Betroffene ist dabei auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Regelung in § 4 Abs. 3 ThürDSG korrespondiert mit § 19 Abs. 3 ThürDSG, wonach der Betroffene, wenn Daten bei ihm selbst erhoben werden, auf die konkrete Rechtsvorschrift, auf seine Mitwirkungspflicht bei der Gewährung von Rechtsvorteilen oder die Freiwilligkeit seiner Angaben hinzuweisen

ist. Eine Einwilligung wird nur dann rechtswirksam erteilt, wenn der Einwilligende die Bedeutung und Tragweite seiner Entscheidung zu überblicken vermag. Bei der Formulierung der Einwilligungserklärung ist dies zu berücksichtigen.

Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist die Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben (z. B. durch Fettdruck, Umrahmung der Erklärung).

4.4 § 4 Abs. 4 ThürDSG konkretisiert den in § 4 Abs. 3 Satz 2 ThürDSG enthaltenen unbestimmten Rechtsbegriff „besondere Umstände“ und trägt damit einem Bedürfnis der empirischen Forschung Rechnung. Die Regelung berücksichtigt, dass eine schriftliche Einholung der Einwilligung durch die Forschung – z. B. bei Umfragen zur Meinungs- und Marktforschung, bei Verkehrsbefragungen und anderen Erhebungen - vielfach nicht möglich ist. An die Stelle des Schriftformerfordernisses treten die hier genannten Dokumentationspflichten.

4.5 Absatz 5 setzt die in Artikel 8 Abs. 1 der EG-Datenschutzrichtlinie enthaltenen Vorgaben zur Verarbeitung besonderer Kategorien personenbezogener Daten (grundsätzliches Verbot der Verarbeitung mit Erlaubnisvorbehalt) in eine praxisgerechte Formulierung um. Der Katalog der sensiblen Daten ist wörtlich aus der EG-Datenschutzrichtlinie übernommen; die Voraussetzungen, unter denen die als sensibel anzusehenden Daten verarbeitet oder genutzt werden dürfen, werden abschließend aufgezählt. Es ist also nicht zulässig, andere Datenkategorien, die weithin als ähnlich sensibel empfunden werden (etwa Daten über wirtschaftliche Verhältnisse), denselben Regeln zu unterwerfen.

Nummer 1:
Eine Rechtsvorschrift ist nur dann ausreichend, wenn sie ausdrücklich die Verarbeitung der abschließend aufgezählten, besonders geschützten Daten erlaubt. In der Regel werden sie also im Wortlaut der Rechtsvorschrift genannt sein müssen. Die zweite Alternative stellt auf (ältere) Rechtsvorschriften ab, die den Umgang mit diesen Daten zwar nicht ausdrücklich regeln, aber zwingend voraussetzen.

Nummer 2:
Einer Einwilligung muss klar zu entnehmen sein, dass sie sich (nur oder auch) auf sensible Daten erstreckt.

Nummer 3:
Ist der Betroffene oder der Dritte zu einer Einwilligung gemäß Nummer 2 physisch oder rechtlich nicht im Stande, kann ausnahmsweise zum Schutz lebenswichtiger Interessen die Verarbeitung oder Nutzung zulässig sein. Die ausnahmsweise zulässige Verarbeitung oder Nutzung kommt nur dann in Betracht, wenn anzunehmen ist, dass die betroffenen Personen einwilligen würden, wenn sie zu einer Entscheidung in der Lage wären (mutmaßliche Einwilligung).

Nummer 4:
Die Offenkundigkeit von Daten genügt für sich allein nicht; sie muss vielmehr auf ein eigenes Handeln des Betroffenen zurückzuführen sein.

Nummer 5:

Als Generalklausel ausgestattet gewährleistet diese Vorschrift, dass sensible Daten zur Abwehr bestimmter Gefahrensituationen verarbeitet oder genutzt werden dürfen.

Nummer 6:
Die Bestimmung erlaubt, sensible Daten im Rahmen des Erforderlichen zu Forschungszwecken zu verarbeiten oder zu nutzen. Sie stellt sicher, dass die Forschung unter den hier aufgestellten Voraussetzungen auch auf sensible Daten zurückgreifen kann.

Nummer 7:
Die Bestimmung unterstreicht, dass das Erforderlichkeitsprinzip bei der Verarbeitung oder Nutzung sensibler Daten im Rahmen von Dienst- und Arbeitsverhältnissen zu beachten ist. Zu den Pflichten, zu deren Erfüllung diese Datenverarbeitung erforderlich sein kann, gehört besonders der Gesundheitsschutz am Arbeitsplatz.

Nummer 8:
Die Verarbeitung oder Nutzung sensibler Daten im medizinischen Sektor ist unter Erforderlichkeitsgrundsätzen entsprechend den hier genannten Maßgaben zulässig.

4.6 Die EG-Datenschutzrichtlinie schreibt vor, dass der Betroffene zumindest in einigen aufgezeigten Fällen ein Widerspruchsrecht gegen die Verarbeitung seiner Daten erhalten muss, wenn der Verarbeitung überwiegende schutzwürdige Gründe aus seiner besonderen Situation entgegenstehen. Aus der Begründung der EG-Datenschutzrichtlinie ergibt sich eindeutig, dass dieses Recht jede betroffene Person besitzen soll, „auch wenn die Daten Gegenstand einer rechtmäßigen Verarbeitung aufgrund eines öffentlichen Interesses oder der Ausübung hoheitlicher Gewalt“ sind. Es geht also nicht darum, auf Wunsch des Betroffenen die Rechtmäßigkeitsvoraussetzungen nochmals zu überprüfen, sondern unabhängig davon, zusätzliche Überlegungen aufgrund der besonderen persönlichen Lage des Betroffen anzustellen. Absatz 6 setzt dieses Recht um.

Ein derartiges Widerspruchsrecht aus persönlichen Gründen gegen ein rechtmäßiges Verwaltungshandeln ist dem deutschen Verwaltungsverfahrensrecht fremd; der Widerspruch ist nicht mit dem im Verwaltungsprozessrecht geregelten Widerspruch gleichzusetzen. Um eine Verwechslung mit dem in der Verwaltungsgerichtsordnung geregelten Widerspruch zu vermeiden, wurde dieser besetzte Begriff bewusst nicht verwendet (siehe § 5 Abs. 1 Nr. 7 ThürDSG).

Die Anwendungsfälle dürften gering sein. Denkbar ist z. B. das Verlangen eines Betroffenen, einen Vorgang, der seine höchstpersönlichen Daten zum Gegenstand hat, nicht vom zuständigen Bediensteten bearbeiten zu lassen, weil dieser zu seinem Bekanntenkreis gehört, ohne zugleich den Tatbestand der Befangenheit im Sinne des Verwaltungsverfahrensrechts zu erfüllen.

Kommt die Behörde bei der gebotenen Abwägung zu dem Ergebnis, dass die vorgetragenen besonderen persönlichen Gründe das öffentliche Interesse an der Verarbeitung oder Nutzung überwiegen, muss diese unterbleiben oder so gestaltet werden, wie es dem Anliegen des Betroffenen entspricht. Das Ergebnis der Abwägung ist dem Betroffenen schriftlich mit Begründung mitzuteilen. Gegen eine ablehnende

Entscheidung kann er Widerspruch nach den Regeln des Verwaltungsprozessrechts einlegen.

Artikel 14 Buchstabe a der EG-Datenschutzrichtlinie lässt ohne Bedingungen einen Verzicht auf den Widerspruch gegen eine rechtmäßige Datenverarbeitung zu, wenn eine im einzelstaatlichen Recht vorgesehene Bestimmung entgegensteht. Daher bestimmt Satz 3, dass das Widerspruchsrecht nicht gilt, wenn eine Rechtsvorschrift die Verarbeitung oder Nutzung zwingend anordnet. So kann die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung (z. B. Pflicht der Meldebehörden zur Führung des Melderegisters) erforderlich sein.

4.7 Nach Artikel 3 Abs. 2, 1. Anstrich EG-Datenschutzrichtlinie sind Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich generell von den Richtlinienregelungen ausgenommen. Inwieweit zu den in Absatz 7 genannten Zwecken besonders geschützte Daten verarbeitet oder genutzt werden dürfen, bestimmt sich nach den hierfür einschlägigen Gesetzen. Absatz 7 nimmt daher diese Aufgabenbereiche ausdrücklich von den Regelungen des § 4 Abs. 5 und 6 ThürDSG aus. Eine Einschränkung im Anwendungsbereich für Gerichte hinsichtlich nicht automatisierter Verarbeitung ist mit Blick auf die Besonderheiten der Verarbeitung besonders geschützter Daten in Gerichtsverfahren gerechtfertigt. Gleiches gilt für die Regelung nach Absatz 6, da die Erhebung von Einwänden in einem laufenden Gerichtsverfahren im Interesse der Rechtsfindung nicht vorstellbar erscheint und die Abwägungen überdies das Funktionieren der Rechtsprechung behindern würden.

Zu § 5 ThürDSG

Die Regelung in § 5 ThürDSG fasst die in den §§ 10 bis 18 ThürDSG sowie die in den §§ 4 Abs. 6 und 5a ThürDSG näher beschriebenen Rechte des Betroffenen zusammen (Absatz 1) und legt fest, dass diese Rechte nicht im voraus durch Rechtsgeschäft (d. h. durch Verzicht als einseitiges Rechtsgeschäft oder durch Vertrag) ausgeschlossen oder beschränkt werden können (Absatz 2). Diese Einschränkung der Dispositionsfreiheit erfolgt im Interesse des Betroffenen.

Die Regelung in Absatz 3 soll sicherstellen, dass der Betroffene auch bei im Verbund betriebenen Verfahren und bei vernetzten Systemen seine Rechte, ohne komplizierte Nachforschungen anstellen zu müssen, wirksam geltend machen kann.

Mit Absatz 4 wurde erstmals eine Regelung für Chipkarten und andere datenverarbeitungstechnische Entwicklungen dieser Art geschaffen. Die Begriffsbestimmung ist so umfassend, dass (voraussichtlich) alle künftigen Neuerungen auf diesem Gebiet erfasst werden. Ihnen ist gemeinsam, dass dem Betroffenen ein Datenträger beliebiger Beschaffenheit zur Verfügung gestellt wird, auf dem seine Daten verarbeitet werden.

Die Daten verarbeitende, den Datenträger herausgebende Stelle hat den Inhaber des Datenträgers ausreichend über seine Rechte zu unterrichten. Sie hat technische Einrichtungen zur Verfügung zu stellen, damit der Betroffene ohne unvertretbaren Aufwand feststellen kann, welche Daten jeweils über ihn gespeichert sind.

Zu § 5a ThürDSG
Die Regelung in § 5a ThürDSG dient der Umsetzung von Artikel 15 der EG-Datenschutzrichtlinie. Entscheidungen, die auf einer Bewertung des Betroffenen beruhen und damit sein Persönlichkeitsrecht im Kern berühren, dürfen vorbehaltlich einer anders lautenden gesetzlichen Regelung oder Vereinbarung zwischen der Daten verarbeitenden Stelle und dem Betroffenen nicht allein einer technischen Vorrichtung überlassen werden, sondern müssen letztlich immer von einer natürlichen Person verantwortet werden. Die Bestimmung soll verhindern, dass Entscheidungen aufgrund von Persönlichkeitsprofilen ergehen, ohne dass der Betroffene die Möglichkeit hat, die zugrunde liegenden Angaben und Bewertungsmaßstäbe zu erfahren. Dabei ist darauf zu achten, dass bei einer Vereinbarung zwischen der Daten verarbeitenden Stelle und dem Betroffenen diese nicht unter etwaigen Zwang zustande gekommen sein darf.

Zu § 6 ThürDSG
Wer bei öffentlichen Stellen beschäftigt ist, hat das Datengeheimnis zu wahren: Es ist untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen. Dienstliche Daten dürfen insbesondere nur zur rechtmäßigen dienstlichen Aufgabenerfüllung verwendet werden und nicht für andere (z. B. private) Zwecke. Ein Verstoß gegen das Datengeheimnis kann bei Beamten disziplinarische Maßnahmen zur Folge haben, bei Angestellten und Arbeitern stellt dies einen Verstoß gegen arbeitsvertragliche Pflichten dar, deren Folgen z. B. Abmahnung oder Kündigung sein können. Den Beschäftigten, die entgegen § 6 ThürDSG personenbezogene Daten verarbeiten oder nutzen, droht zumindest bei vorsätzlichem Handeln darüber hinaus eine strafrechtliche Verfolgung nach § 43 ThürDSG oder § 203 StGB. Die Beschäftigten sind bei Arbeitsaufnahme sowie aus besonderem Anlass auf diese besonderen Verschwiegenheitspflichten hinzuweisen.

Zu § 7 ThürDSG
7.1 Diese Vorschrift regelt die Zulässigkeit und das Verfahren von sogenannte Online-Anschlüssen dritter Stellen (andere Behörden). Ein solches Verfahren darf nur eingerichtet werden, wenn dies nach Abwägung der schutzwürdigen Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Die Angemessenheit kann sich insbesondere aus der Häufigkeit oder der Dringlichkeit der Abrufe ergeben. Nicht betroffen sind Online-Verfahren, bei denen keine personenbezogenen Daten - sondern z. B. statistische Daten - übermittelt werden. Keine Anwendung findet die Vorschrift ferner in Fällen, in denen zwischen Auftraggeber und Auftragnehmer Daten zugeleitet oder abgerufen werden.

Besondere Berufs- oder Amtsgeheimnisse im Sinne von § 7 Abs. 1 Satz 2 ThürDSG sind insbesondere in § 203 Abs. 1 StGB genannt; dieser Vorschrift unterliegen z. B. Ärzte, Apotheker, Angehörige sonstiger Heilberufe, Berufspsychologen, Rechtsanwälte, Notare, Ehe-, Erziehungs- und Jugendberater und staatlich anerkannte Sozialarbeiter.

7.2 In Korrespondenz mit § 10 ThürDSG regelt Absatz 2 die Dokumentationspflicht, die für mögliche Datenschutzkontrollen sowie für die nach Absatz 3 notwendige

Unterrichtung erforderlich ist. Die Festlegungen gemäß Nummer 2 und 3 werden im Verfahrensverzeichnis unter Ziff. 4.1 und 4.4 dokumentiert.

7.3 Die Unterrichtung des TLfD nach § 7 Abs. 3 ThürDSG hat so rechtzeitig zu erfolgen, dass dieser noch Gelegenheit hat, die Zulässigkeit des Verfahrens vor dessen endgültiger Festlegung zu überprüfen. Nach § 7 Abs. 3 Satz 2 ThürDSG bedarf die Einrichtung eines Abrufverfahrens, an dem Staatsanwaltschaften, Polizeibehörden, Verfassungsschutzbehörden, der Bundesnachrichtendienst, der Militärische Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministers der Verteidigung, beteiligt sind, der Zustimmung des für die Daten verarbeitende und die abrufende Stelle jeweils zuständigen Ministeriums. Die Bestimmungen zur Freigabe von automatisierten Verfahren (§ 34 ThürDSG) sind zu beachten.

7.4 § 7 Abs. 4 ThürDSG stellt klar, dass die materiell rechtliche Zulässigkeit des einzelnen Abrufs nach den §§ 19 ff. ThürDSG zu beurteilen ist. Ferner wird festgelegt, dass die Verantwortung für die Zulässigkeit des einzelnen Abrufs beim Empfänger liegt. Dabei wird berücksichtigt, dass die Daten verarbeitende Stelle vom Abruf personenbezogener Daten im Rahmen eines Abrufverfahrens regelmäßig keine Kenntnis erlangt. Eine Prüfungspflicht für die Daten verarbeitende Stelle besteht nur, wenn Hinweise für ein mögliches Fehlverhalten der abrufenden Stelle vorliegen. Mit der Einrichtung von Abrufverfahren hat die Daten verarbeitende Stelle durch die Protokollierung der Abrufe - zumindest durch ein geeignetes Stichprobenverfahren - zu gewährleisten, dass eine Überprüfung der vorgenommenen Datenübermittlungen auf ihre Rechtmäßigkeit möglich ist.

7.5 Nach § 7 Abs. 5 ThürDSG gelten die Absätze 1 bis 4 indes nicht für jedermann zugängliche Datenbestände (z. B. Autorenverzeichnis einer öffentlichen Bibliothek).

7.6 Die Bestimmungen zum automatisierten Abrufverfahren sind - mit Ausnahme der Unterrichtung des TLfD und der Einholung der Zustimmung des jeweils zuständigen Ministeriums - auch innerhalb öffentlicher Stellen zu beachten, um dem Grundsatz der Zweckbindung und Verhältnismäßigkeit Rechnung zu tragen.

Zu § 8 ThürDSG

Datenverarbeitung im Auftrag im Sinne des § 8 ThürDSG umfasst jene Fälle, in denen die tatsächliche Verarbeitung personenbezogener Daten für eine andere Stelle erfolgt, der Auftraggeber aber für die Verarbeitung und deren Ergebnisse nach außen verantwortlich bleibt. Die Weitergabe an die Auftragnehmer stellt keine Datenübermittlung dar. Bedienen sich öffentliche Stellen zur Erledigung ihrer Aufgaben gemeinsamer Rechenzentren oder Rechenzentren anderer öffentlicher oder privater Stellen, liegt Auftragsdatenverarbeitung vor. Auftragsdatenverarbeitung liegt auch bei externer Datenerhebung, Datenerfassung auf Datenträgern, Mikroverfilmung von Unterlagen, Vernichtung von Schriftgut und Datenträgern sowie bei der Auftragsarchivierung vor.

Abzugrenzen von der Datenverarbeitung im Auftrag ist die sogenannte Funktionsübertragung, bei der nicht lediglich die Durchführung der Verarbeitung oder Nutzung, sondern die Aufgabe selbst, zu deren Wahrnehmung die Verarbeitung oder Nutzung

dient, auf eine andere Stelle übertragen wird (z. B. die Übertragung einer Aufgabe auf ein beliehenes Unternehmen). Eine solche Funktionsübertragung – auch Outsourcing genannt – bedarf einer Rechtsgrundlage.

Für personenbezogene Daten, die besonderen Geheimhaltungsbestimmungen, Berufs- oder besonderen Amtsgeheimnissen unterliegen, gelten Einschränkungen für die Auftragsdatenverarbeitung. Die Auftragsdatenverarbeitung von Sozialdaten (z. B. Sozialhilfe, Jugendhilfe, Wohngeld) ist nach § 80 Abs. 5 SGB X nur in erheblich eingeschränktem Umfang zulässig. Die Verarbeitung durch nicht öffentliche Stellen ist nur zulässig, wenn anders Störungen im Betriebsablauf nicht vermieden oder Teilvorgänge der automatischen Datenverarbeitung hierdurch erheblich kostengünstiger besorgt werden können. Dies ist z. B. der Fall, wenn Verfahren, wie die Mikroverfilmung, das Vorhandensein kostenträchtiger Technik voraussetzen.

Angehörige von Behörden, die besonderen, durch § 203 Abs. 1 StGB geschützten Verschwiegenheitspflichten unterliegen (insbesondere Amtsärzte, bei öffentlichen Stellen beschäftigte Ehe-, Erziehungs- und Jugendberater sowie staatlich anerkannte Sozialarbeiter) dürfen die ihnen anvertrauten personenbezogenen Daten Dritten nur offenbaren, wenn sie hierzu i. S. v. § 203 Abs. 1 StGB befugt sind (sog. Offenbarungsbefugnis). Eine nach Maßgabe dieses Gesetzes erklärte Einwilligung kann eine Befugnis begründen (vgl. hierzu Urteil des BGH vom 10.07.1991 zur Einschaltung ärztlicher Verrechnungsstellen). Eine Auftragsdatenverarbeitung ohne Einwilligung des Betroffenen ist insoweit ausgeschlossen, als die für die Auftragserledigung erforderliche Datenweitergabe an den Auftragnehmer eine unzulässige Offenbarung darstellt.

8.1 Nach § 8 Abs. 1 ThürDSG bleibt die Stelle, die sich zur Erfüllung ihrer Aufgaben der verarbeiteten Daten bedient, für die Einhaltung der Vorschriften des Gesetzes auch dann verantwortlich, wenn die Daten in ihrem Auftrag durch andere Personen oder Stellen verarbeitet werden. Dabei hat sie ganz konkret in schriftlichen Vereinbarungen und Weisungen Art und Umfang der Datenverarbeitung und -nutzung dem Auftragnehmer vorzugeben und dies zu kontrollieren. Eine Verfahrensweise, wonach der Auftraggeber lediglich den Auftragnehmer in allgemeiner Form beauftragt und der Auftragnehmer faktisch Art, Umfang und Rahmenbedingungen der Datenverarbeitung bestimmt, ist nicht mit § 8 ThürDSG vereinbar. Welcher Art die Rechtsbeziehungen zwischen Auftraggeber und Auftragnehmer sind, ist dabei unbeachtlich. Ansprüche auf Auskunft, Berichtigung, Sperrung und Löschung sind daher gegen die auftraggebende Stelle zu richten.

8.2 Der Auftragnehmer ist anhand der von ihm getroffenen Datensicherheitsmaßnahmen (§ 9 ThürDSG) sowie der Maßnahmen zur Wahrung des Datengeheimnisses (§ 6 ThürDSG) sorgfältig auszuwählen. Die Auftragserteilung hat schriftlich zu erfolgen und zugleich Festlegungen zur Duldungspflicht des Auftragnehmers hinsichtlich vom Auftraggeber veranlasster Kontrollen zu enthalten. Neben den festzulegenden technischen und organisatorischen Maßnahmen zur Datensicherheit sind gleichfalls Vereinbarungen darüber zu treffen, ob und inwieweit Unterauftragsverhältnisse zulässig sind bzw. wie im Havariefall zu verfahren ist. Darüber hinaus sollten die Vereinbarungen Festlegungen zur Verfahrensweise bei festgestellten Verstößen gegen den Datenschutz und die Datensicherheit (z. B. Sofortkündigungsrecht) sowie zur Unterstützung von Kontrollen durch den Auftraggeber unter

Berücksichtigung der Kontrollrechte des TLfD gegenüber dem Auftraggeber enthalten. Insofern werden die Rahmenbedingungen bei der Auftragserteilung festgelegt.

Da der Auftraggeber nach § 8 Abs. 1 ThürDSG in allen Phasen der Auftragsdurchführung für die Sicherstellung des Datenschutzes verantwortlich bleibt, muss er sich (ggf. vor Ort) überzeugen, ob die nach § 9 ThürDSG gebotenen und im Auftrag festgelegten technisch-organisatorischen Maßnahmen auch tatsächlich umgesetzt und beachtet werden. Die seitens des Auftragnehmers jederzeit zu ermöglichenden Kontrollen sollen in Abhängigkeit der dem Auftrag zugrundeliegenden Sensibilität der Daten unter Beachtung des Grundsatzes der Erforderlichkeit erfolgen. Als zwingend wird eine Kontrolle vor Ort durch den Auftraggeber dann anzusehen sein, wenn beispielsweise Beschwerden oder andere Anhaltspunkte vorliegen, dass datenschutzrechtliche Maßgaben durch den Auftragnehmer nicht eingehalten werden. Neben einer Kontrolle vor Ort durch den Auftraggeber kann auch eine Information der für den Auftragnehmer zuständigen Datenschutzkontrollstelle geeignet sein, Abhilfe zu schaffen.

Absatz 2 Satz 5 erlaubt auch, dass die Fachaufsicht zentral einen Auftrag für die ihrer Aufsicht unterfallenden Stellen erteilt.

8.3 In § 8 Abs. 3 ThürDSG wird dem Auftragnehmer eine Hinweispflicht auferlegt, wenn er der Ansicht ist, dass die Verarbeitung gegen datenschutzrechtliche Bestimmungen verstößt. Die Regelung trägt dem Umstand Rechnung, dass der Auftragnehmer in einer Reihe von Fällen infolge des täglichen Umgangs mit datenschutzrechtlichen Fragen eher als der Auftraggeber in der Lage ist, die Gesetzeskonformität von Weisungen zu beurteilen.

8.4 § 8 Abs. 4 ThürDSG findet nur Anwendung, wenn eine öffentliche Stelle des Freistaates als Auftragnehmer Daten verarbeitet oder nutzt. Nur für diesen Fall steht dem Landesgesetzgeber die Gesetzgebungskompetenz zu. Da der Auftragnehmer in dieser Funktion nicht selbst Daten verarbeitende Stelle ist, kommen für ihn nur die in Absatz 4 bezeichneten Bestimmungen des Gesetzes zur Anwendung. Hiernach obliegt ihm auch, einen Beauftragten für den Datenschutz nach § 10a ThürDSG zu bestellen.

8.5 Soweit das Land oder eine der Aufsicht des Landes unterstehende Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts die Mehrheit der Anteile oder die Mehrheit der Stimmen bei einem Auftragnehmer besitzt, der indes keine öffentliche Stelle im Sinne des ThürDSG (siehe Ziff. 2.1) darstellt, gelten die in § 8 Abs. 5 ThürDSG genannten Bestimmungen des ThürDSG entsprechend. Die bezeichneten Mehrheitsverhältnisse rechtfertigen für diesen speziellen Fall der Auftragsdatenverarbeitung eine Bezugnahme auf das ThürDSG.

8.6 Auftragnehmer, auf die die Bestimmungen des ThürDSG nicht anwendbar sind, können private und damit nicht öffentliche Stellen des Freistaates, öffentliche und nicht öffentliche Stellen in anderen Bundesländern sowie Stellen in den Mitgliedsstaaten der Europäischen Union sein.

Für die Beauftragung privater Unternehmen (nicht öffentlicher Stellen) gilt grundsätzlich Folgendes:
Eine Beauftragung privater Unternehmen soll nur erfolgen, wenn und solange dies

zur Aufrechterhaltung eines geordneten Dienstbetriebes unerlässlich ist. Langfristig ist anzustreben, dass hoheitliche Aufgaben - wozu auch das Verarbeiten zwangsweise von den Betroffenen erhobener Daten zählt - durch die Daten verarbeitenden Stellen selbst oder durch andere öffentliche Stellen, die der Aufsicht des Landes Thüringen unterliegen, wahrgenommen werden.

Insbesondere mit der Verarbeitung von Daten des Melderegisters dürfen private Unternehmen nur beauftragt werden, wenn das Innenministerium zugestimmt hat (vgl. § 37 Abs. 1 ThürMeldeG).

Nach Artikel 17 Abs. 3, 2. Anstrich der EG-Datenschutzrichtlinie gelten für den Auftragsverarbeiter die gleichen Maßgaben für die Sicherheit der Verarbeitung, wie für den für die Verarbeitung Verantwortlichen. Maßgebend sind hierbei die Rechtsvorschriften des Mitgliedsstaats, in dem er seinen Sitz hat. Absatz 6 folgt diesem Rechtsgedanken; mittels der hier vorgesehenen Unterrichtung durch den Auftraggeber wird die für den Auftragnehmer zuständige Kontrollstelle befähigt, die Auswahl sowie Einhaltung der technischen und organisatorischen Maßnahmen beim Auftragnehmer zu kontrollieren.

Handelt es sich um einen Auftragnehmer innerhalb Thüringens, ist die Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich nach § 38 BDSG, das Thüringer Landesverwaltungsamt, über die Beauftragung zu unterrichten. Handelt es sich um einen Auftragnehmer außerhalb Thüringens, muss die in dessen Land zuständige Kontrollstelle unterrichtet werden (z. B. bei Bundesbehörden = Bundesbeauftragter für den Datenschutz; bei öffentlichen Stellen in anderen Bundesländern = Landesbeauftragter für den Datenschutz des jeweiligen Bundeslandes; bei Privatunternehmen in der Bundesrepublik = zuständige Aufsichtsbehörde für den nicht öffentlichen Bereich des jeweiligen Bundeslandes; bei Behörden, Betrieben und Einrichtungen im Ausland = zuständige Kontrollstelle für den Datenschutz des jeweiligen Landes).

Da der Auftraggeber auch im Falle einer Auftragsdatenverarbeitung für die Gewährleistung des Datenschutzes und der Datensicherheit bezüglich der zugrunde liegenden Datenverarbeitung verantwortlich bleibt und die Betroffenenrechte wie Auskunft, Schadensersatz, ect. ihm gegenüber geltend zu machen sind, bleibt ihm unbenommen, sich (insbesondere bei Zweifelsfragen) im Falle beabsichtigter Auftragsdatenverarbeitung an den TLfD (siehe § 40 ThürDSG) oder an das für Grundsatzfragen des Datenschutzrechts zuständige Ressort der Landesregierung zu wenden.

8.7 Die Regelung erfasst vornehmlich die praktisch wichtige Konstellation der Fernwartung mit Hilfe der Datenfernübertragung. Sie findet aber auch dann Anwendung, wenn Prüfung oder Wartung vor Ort beim Anwender durch einen externen Techniker erfolgen. In den aufgezeigten Fällen stellt die Prüfung oder Wartung automatisierter Datenverarbeitungsanlagen – in der Regel – keine Auftragsdatenverarbeitung dar, da es an der Zielrichtung, die gespeicherten Daten zur Verarbeitung oder Nutzung ihres Informationsgehaltes zu überlassen, fehlt.

Indem § 8 Abs. 7 ThürDSG die Absätze 1 bis 5 auch für o.g. Fälle für entsprechend anwendbar erklärt, werden die Belange der Betroffenen auch im Falle der Vornahme von Wartungsarbeiten und damit der Einschaltung Dritter ausreichend gewahrt.

Bezüglich der Kenntnisnahme von Daten, die besonderen Geheimhaltungsbestimmungen unterliegen, gilt das in den einleitenden Bemerkungen zu § 8 ThürDSG Ausgeführte entsprechend.

Zu § 9 ThürDSG

9.1 Öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten verarbeiten, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des ThürDSG und anderer Vorschriften des Datenschutzes zu gewährleisten. Die Verpflichtung zur Durchführung von Datensicherheitsmaßnahmen gilt für die automatisierte und nichtautomatisierte Datenverarbeitung (also z. B. auch für manuelle Karteien und Akten). Dabei gilt der Grundsatz der Verhältnismäßigkeit. Unter Berücksichtigung des Standes der Technik haben Maßnahmen ein Schutzniveau zu gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. Muss aus Gründen des Angemessenheitsprinzips auf eine bestimmte Maßnahme verzichtet werden, so ist dies nachvollziehbar zu dokumentieren. Von daher sind alle auf ein Verfahren bezogenen Maßnahmen in ihrer Gesamtheit zu betrachten; die Summe der zu treffenden Maßnahmen muss die notwendige Sicherheit gewährleisten.

9.2 Die starke Technologieabhängigkeit konkreter technischer und organisatorischer Maßnahmen muss in immer kürzeren Abständen zu deren Anpassung an die technische Entwicklung führen. Maßnahmen müssen sich zugleich dem Einzelfall anpassen und sind vom Schutzbedarf der Daten, vom Verarbeitungssystem, von der Bedrohungslage und vom Stand der Technik abhängig. Sie stehen in einem engen sachlichen Zusammenhang mit der Datensicherheit (IT-Sicherheit) im Bereich der automatisierten Datenverarbeitung.

Das Gesetz schreibt vor, auf der Grundlage eines Sicherheitskonzeptes die technischen und organisatorischen Maßnahmen zu ermitteln und formuliert die am Schutzbedarf der Daten ausgerichteten Sicherheitsziele. Damit ist die Aufgabe verbunden, nach der Art der Daten zunächst deren Schutzbedarf festzustellen. Als Hilfsmittel für die Einstufung personenbezogener Daten nach dem Grad ihrer Sensibilität und für die Festlegung von Schutzzielen in Abhängigkeit vom Grad der Beeinträchtigung des informationellen Selbstbestimmungsrechts bei einem etwaigen Mißbrauch bietet sich folgendes **Schutzstufenkonzept** an:

Stufe 0: Kein besonderer Schutzbedarf

Personenbezogene Daten aus öffentlich zugänglichen Quellen, deren Verarbeitung keine Beeinträchtigung des informationellen Selbstbestimmungsrechtes erwarten lässt und die in Bezug auf Änderungen, Verfälschungen etc. keines besonderen Schutzes bedürfen.

Beispiele: Angaben aus öffentlichen Telefon- und Adreßbüchern, Branchenverzeichnissen, amtliche Bekanntmachungen, Presseveröffentlichungen.

Stufe 1: Grundschutzbedarf

Personenbezogene Daten, deren Verarbeitung eine Beeinträchtigung des infor-

mationellen Selbstbestimmungsrechts insofern erwarten lässt, als durch einen Missbrauch der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.

Beispiele: Daten, deren Übermittlung eines berechtigten Interesses bedürfen, z. B. Daten aus öffentlichen Registern (Grundbuchauskunft, erweiterte Melderegisterauskunft - sofern keine Auskunftssperre vorliegt, u. ä.).

Stufe 2: Hoher Schutzbedarf
Personenbezogene Daten, deren Verarbeitung eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts insofern erwarten läßt, als der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann oder personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen oder deren unbefugte Kenntnis eine Gefahr für Leib, Leben oder die persönliche Freiheit des Betroffenen befürchten lässt.

Beispiele: Daten, deren Übermittlung eines rechtlichen Interesses bedürfen; Sozial-; Gesundheits-; Steuer-; Personaldaten; Daten zu religiösen und politischen Anschauungen; Daten, die Berufs- und Geschäftsgeheimnisse sowie das Fernmeldegeheimnis betreffen; personenbezogene Daten von Personen, deren Identität zu schützen ist.

Soweit seitens des Interministeriellen Ausschusses Informationstechnik (IMA-IT) bzw. des zuständigen Ministeriums keine verbindlichen methodischen Vorgaben für Sicherheitskonzepte existieren, wird empfohlen, die Erarbeitung nach den Regeln des „IT-Grundschutzhandbuchs“ vorzunehmen, das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn herausgegeben und ständig weiterentwickelt wird (Bundesanzeiger-Verlag/Loseblattsammlung und auf CD-ROM). Bei einem hohen Schutzbedarf ist zusätzlich zu prüfen, ob neben den Standardsicherheitsmaßnahmen gemäß IT-Grundschutzhandbuch spezifische Maßnahmen erforderlich sind.

Die bisher im Datenschutzrecht des Bundes und der Länder formulierten Maßnahmen hatten als „Gebote der Datensicherheit“ im Wesentlichen die technischen Komponenten von Datenverarbeitungsanlagen zum Gegenstand. Sie gehören unverändert zum bewährten Instrumentarium der Datensicherheit und sind grundsätzlich geeignet, wesentlich zur Erfüllung der Schutzziele des § 9 Abs. 2 ThürDSG beizutragen. Nachfolgend werden daher wesentliche Maßnahmen zur Gewährleistung der Datensicherheit genannt:

1. Zutrittskontrolle
Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Beispiele für Maßnahmen:
- Anlagen, PC und Terminals nicht an allgemein zugänglichen Orten aufstellen,
- keine Hinweise auf Rechenzentren, Verteileranlagen usw.,
- Abschließen der Räume mit DV-Anlagen oder -Terminals,
- Festlegung von Zutrittsbefugnissen,

- Regelung für Besucher, Reinigungsdienst, Wartung, Abschließen der Geräte, verschlossene Aufbewahrung der Datenträger,
- Fenster- und Türensicherung durch Spezialglas, einbruchhemmende Türen,
- Installation von Überwachungsanlagen, Überwachungspersonal.

2. Zugangskontrolle
Die Benutzung von Datenverarbeitungssystemen durch Unbefugte ist zu verhindern.

Beispiele für Maßnahmen:
- Begrenzung der Zugangsberechtigten,
- Abweisung unberechtigter Nutzer mit Protokollierung der Zugangsversuche,
- Begrenzung fehlerhafter Zugangsversuche,
- Vorgaben zur Passwortgestaltung, -handhabung und –verwaltung,
- Dunkelschaltung des Bildschirms mit Passwortschutz,
- Einsatz von Identifikations- und Authentifikationsverfahren,
- Überwachung von Netzwerkzugängen (Einsatz von Firewalls),
- Besondere Absicherung bei Fremd- und Fernwartung,
- Verzicht auf Zugriff über Wählleitung auf sensible Daten.

3. Zugriffskontrolle
Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beispiele für Maßnahmen:
- zeitliche Begrenzung der Zugriffsmöglichkeit,
- Verwendung von sicheren Passwortverfahren, Benutzerkennungen,
- Festlegung und softwaremäßig Absicherung der Zugriffsberechtigungen,
- Protokollierung von Zugriffen und Zugriffsversuchen des Benutzers,
- Verschlüsselung von Daten und Signierung von Programmen,
- Festlegung von Personen, die Datenträger nutzen oder entfernen dürfen,
- Datenträgerverwaltung (schriftliche Regelung über den Umgang mit Datenträgern, automationsgestützte oder manuelle Aufzeichnung über den Verbleib von Datenträgern) mit Kontrollen,
- Einschließen der Datenträger,
- Verbot der Verwendung privater Datenträger im Dienst und der Mitnahme dienstlicher Datenträger nach Hause,
- organisatorische, softwaremäßige und hardwaremäßige Festlegung der Befugnisse zum Kopieren,
- physikalisches Löschen nicht mehr benötigter Daten,
- Einsatz von Sicherheitssoftware,
- Einsatz von Kopierschutzmaßnahmen,
- Vernichtung überflüssiger Ausdrucke und Fehldrucke.

4. Weitergabekontrolle
Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträger

nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beispiele für Maßnahmen:
- Dokumentation von Übermittlungsprogrammen,
- Festlegung der Datenempfänger,
- Protokoll der Übermittlungen,
- Verschlüsselung der zu übertragenden Daten,
- Einsatz der elektronischen Signatur,
- Einsatz von Prüfsummenverfahren,
- Regelung des Kommunikationsverkehrs,
- Prüfung der Identität der empfangenden Stelle hinsichtlich der Zulässigkeit von Übermittlungen.

5. Eingabekontrolle
Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Beispiele für Maßnahmen:
- Protokoll der Eingaben (wer hat wann, was neu aufgenommen, geändert oder gelöscht?),
- Einsatz von Sicherheitssoftware.

6. Auftragskontrolle
Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Beispiele für Maßnahmen:
- sorgfältige Auswahl des Auftragnehmers,
- klare schriftliche Vereinbarungen zwischen Auftraggeber und Auftragnehmer über Rechte und Pflichten der Vertragspartner,
- Kontrolle der Vertragsausführung (insbesondere hinsichtlich der Einhaltung der Datensicherheitspflichten),
- Vereinbarung von Vertragsstrafen und arbeitsrechtlichen Maßnahmen bei Nichteinhalten der Pflichten,
- Genehmigung von Subunternehmen.

7. Verfügbarkeitskontrolle
Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Beispiele für Maßnahmen:
- regelmäßige Datensicherungen, Sicherheitskopien an einem anderen Ort,
- Einsatz gespiegelter Festplatten oder RAID-Systeme,
- unterbrechungsfreie Stromversorgung,
- Maßnahmen zum Katastrophenschutz,

– Dokumentation der Verarbeitungsprogramme,
– Einsatz von Virenerkennungsprogrammen,
– Schulung der Mitarbeiter.

8. Trennungsgebot
Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beispiele für Maßnahmen:
– getrennte Vorhaltung und getrennte Verarbeitung der Daten,
– Festlegung eines Zulässigkeitsrahmens für die Datenverarbeitung,
– Autorisierung/Rechteverwaltung,
– Protokollierung/Beweissicherung.

Zu § 10 ThürDSG
10.1 Das Verzeichnis der automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, dient der Eigenkontrolle der Behörde und als Grundlage für die Kontrollen des TLfD. Es dient darüber hinaus der Transparenz der Datenverarbeitung innerhalb der öffentlichen Stelle.
Entsprechend § 10a ThürDSG ist dem Beauftragten für den Datenschutz die Führung des Verzeichnisses und folglich die Zuständigkeit für die Publizität der automatisierten Verfahren als Aufgabe übertragen worden.

10.2 Die Angaben, die nach § 10 Abs. 2 ThürDSG in das Verzeichnis aufzunehmen sind, sind teilweise identisch mit den Festlegungen in der datenschutzrechtlichen Freigabe nach § 34 Abs. 2 und 3 ThürDSG (vgl. Ziff. 34.2). Mit der Freigabe des automatisierten Verfahrens sind die erforderlichen Angaben zum Verfahren unverzüglich ins Verfahrensverzeichnis aufzunehmen. Den Hinweisen zum ThürDSG ist ein Musterformblatt (Anlage 1) und eine Erläuterung für das Verfahrensverzeichnis (Anlage 1a) beigefügt.

10.3 Das Verzeichnis kann mit bestimmten Ausnahmen (Angaben zu den Ziffern 8 und 9, Verfahrensverzeichnisse der Verfassungsschutzbehörden sowie bei Vorliegen von Versagungsgründen nach § 13 Abs. 5 ThürDSG) in Umsetzung von Art. 21 EG-Datenschutzrichtlinie von **jedermann** – nicht nur von dem Betroffenen - gebühren- und auslagenfrei eingesehen werden. Ein berechtigtes oder sogar rechtliches Interesse ist von dem Einsichtnehmenden nicht nachzuweisen.

10.4 Ein Verfahrensverzeichnis für die in Absatz 4 bezeichneten Verfahren ist gesetzlich nicht erforderlich, wenn die Voraussetzungen nach § 34 Abs. 3 Satz 1 Nr. 3 ThürDSG oder § 34 Abs. 3 Satz 2 ThürDSG erfüllt sind und damit eine Freigabepflicht entfällt. Gleichwohl sollte aus Gründen der Transparenz und Nachvollziehbarkeit in den Daten verarbeitenden Stellen eine Übersicht geführt werden, aus der sich ergibt, welche Verfahren, mit denen personenbezogene Daten verarbeitet werden, in der Stelle zum Einsatz kommen (Verfahrensübersicht).

Verfahren nach § 34 Abs. 3 Satz 1 Nr. 3 ThürDSG betreffen Register, deren Führung aufgrund von Rechtsvorschriften vorgesehen ist (z. B. Handelsregister). Verfahren nach § 34 Abs. 3 Satz 2 ThürDSG können von der Aufnahme in das Verfahrens-

verzeichnis ausgenommen werden, da dem Gebot der Transparenz der Verarbeitung hier durch die Rechtsverordnung entsprochen wird. Die Ausnahmeregelung beruht auf Artikel 18 Abs. 3 und Artikel 21 Abs. 3 der EG-Datenschutzrichtlinie.

Zu § 10a ThürDSG

Die Sicherstellung des Datenschutzes nach § 34 Abs. 1 ThürDSG obliegt neben den Ministerien auch den Gemeinden und Gemeindeverbänden sowie den sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und deren Vereinigungen. In Umsetzung der EG-Datenschutzrichtlinie sowie mit Blick auf erforderliche Verwaltungsvereinfachungen bei gleichzeitiger Stärkung der Eigenverantwortung der Daten verarbeitenden Stellen erlaubt die Einführung der obligatorischen Bestellung eines Beauftragten für den Datenschutz bei den öffentlichen Stellen (einschließlich des kommunalen Bereichs) den Wegfall der bislang gegenüber dem TLfD bestehenden Meldepflichten und somit die Auflösung des bei diesem geführten Registers.

10a.1 Nach § 10a Abs. 1 ThürDSG dürfen nur Beschäftigte der jeweiligen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellt werden. Einzige Ausnahme ist die Bestellung eines gemeinsamen Beauftragten mehrerer Stellen entsprechend Absatz 6. Unzulässig ist somit die Bestellung externer Personen (z. B. Rechtsanwälte). Auch Gemeinderatsmitglieder können nicht zum Beauftragten für den Datenschutz bestellt werden, da sie keine "Beschäftigten“ ihrer Gemeinden sind. In der Regel sollen Beauftragte für den Datenschutz diese Funktion neben anderen Funktionen in der öffentlichen Stelle ausüben. Sie sollten dabei mit Blick auf die zu wahrende Unabhängigkeit nicht in Interessenkonflikte mit anderen Funktionen bzw. Tätigkeiten geraten und die notwendige Fachkenntnis in Fragen des Datenschutzes und der Datensicherheit besitzen.

Für die Fälle, in denen in einer Daten verarbeitenden Stelle nur Verfahren im Sinne des § 34 Abs. 3 ThürDSG eingesetzt werden, stellt Absatz 1 Satz 2 klar, dass es einer Bestellung eines Datenschutzbeauftragten nicht bedarf. Die Verantwortung beziehungsweise die Sicherstellung des Datenschutzes (§ 34 Abs.1 ThürDSG) verbleibt insofern beim Leiter der Daten verarbeitenden Stelle. Bei der Anwendung von Verfahren im Sinne § 34 Abs. 3 Satz 1 Nr. 1 und 2 ThürDSG ist in diesem Fall § 10 ThürDSG zu beachten und ein Verfahrensverzeichnis unter Aufnahme dieser Verfahren zu führen.

Notare und beliehene Unternehmen müssen nach Absatz 1 Satz 3 erst dann einen Beauftragten für den Datenschutz einsetzen, wenn sie mindestens fünf Personen bei der automatisierten Verarbeitung oder Nutzung personenbezogener Daten beschäftigen. Maßgeblich ist die Zahl der durchschnittlich Beschäftigten, auch wenn diese nicht vollbeschäftigt sind. Zu den Beschäftigten zählen auch Auszubildende.

10a.2 Der Beauftragte für den Datenschutz ist in seiner Funktion dem Behördenleiter unmittelbar nachgeordnet. Eine Übertragung der Unterstellung im Rahmen des Delegationsrechts auf eine weitere Hierarchieebene zwischen dem Behördenleiter und dem Beauftragten für den Datenschutz ist deshalb unzulässig. Der Beauftragte für den Datenschutz hat den Behördenleiter bei der Ausführung der Vorschriften des

ThürDSG und anderer Vorschriften über den Datenschutz zu unterstützen und zu beraten. Er hat insbesondere

- das Anlagen- und Verfahrensverzeichnis nach § 10 ThürDSG zu führen, soweit er von der Dienststelle mit der Führung beauftragt wird; ansonsten hat ihm die Dienststelle das Verzeichnis zur Verfügung zu stellen,
- bei der Freigabe automatisierter Verfahren nach § 34 Abs. 2 ThürDSG mitzuwirken,
- die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden, zu überwachen,
- bei der Gestaltung von Vordrucken der Behörde mitzuwirken, insbesondere im Hinblick auf § 4 Abs. 2 und § 19 Abs. 3 ThürDSG,
- dem Bürger als Anlaufstelle für Fragen des Datenschutzes im Zusammenhang mit der Behörde zu dienen,
- die Beantwortung von Auskunftsersuchen nach § 13 ThürDSG zu koordinieren,
- Organisationseinheiten in der Behörde über Datensicherheitsmaßnahmen zu beraten.

Der Beauftragte für den Datenschutz hat die Verantwortlichen für die Datenverarbeitung und die Behördenleitung darauf hinzuweisen, wenn bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Behörde nach seiner Auffassung gegen die Vorschriften des ThürDSG oder andere Vorschriften des Datenschutzes verstoßen wird. Ein Weisungsrecht gegenüber den Daten verarbeitenden Stellen steht ihm nicht zu.

10a.3 Die Pflicht der Daten verarbeitenden Stelle, den Beauftragten für den Datenschutz in geeigneter Weise bei der Erfüllung seiner Aufgaben zu unterstützen, ist entsprechend den örtlichen und organisatorischen Gegebenheiten zu erfüllen. Zum Beispiel dürfen festgelegte Zugangsberechtigungen die Tätigkeit des Beauftragten für den Datenschutz nicht behindern. Es sind Regelungen innerhalb der jeweiligen Stelle zu treffen, die eine Beteiligung in Angelegenheiten mit datenschutzrechtlichem Charakter gewährleisten. Die erforderlichen Sachmittel und Räumlichkeiten sind seitens der Daten verarbeitenden Stelle zur Verfügung zu stellen.

10a.4 Der Beauftragte für den Datenschutz hat nicht die Befugnis, personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis (Nr. 7.1), insbesondere dem Arztgeheimnis unterliegen, ohne Einwilligung des Betroffenen einzusehen. Entsprechendes gilt auch für Personalakten oder Akten über Sicherheitsüberprüfungen.
Die Verantwortung für die Beachtung der datenschutzrechtlichen Bestimmungen verbleibt auch bei der Bestellung eines Datenschutzbeauftragten bei den für die jeweilige Datenverarbeitung Zuständigen.

10a.5 Die Verschwiegenheitspflicht, die auch das Recht zur Verschwiegenheit umfasst, ist Voraussetzung für die effektive Arbeitsmöglichkeit des Beauftragten für den Datenschutz und gilt nur dann, wenn Beschäftigte der öffentlichen Stelle oder Dritte ihm etwas „anvertrauen“, d.h. freiwillig offenbart haben. Wird der Beauftragte im Einzelfall durch den Betroffenen von dessen Verschwiegenheitspflicht entbunden, kommt dies einer Einwilligung des Betroffenen zur Offenlegung seiner Daten gleich.

10a.6 Nach Absatz 6 können mehrere öffentliche Stellen einen ihrer Beschäftigten zum gemeinsamen Datenschutzbeauftragten bestellen. Dies kann insbesondere zweckmäßig sein, wenn mehrere öffentliche Stellen über eine gemeinsame Verwaltung verfügen. Vor diesem Hintergrund werden Gemeinden und Landkreise sowie Verwaltungsgemeinschaften und Zweckverbände als sonstige der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts unter Aspekten der organisatorischen Zweckmäßigkeit über die Bestellung eines gemeinsamen Datenschutzbeauftragten für mehrere Daten verarbeitende Stellen zu befinden haben. Verwaltungsgemeinschaften und ihre Mitgliedsgemeinden sollen generell einen gemeinsamen Datenschutzbeauftragten bestellen. Gleiches gilt für die erfüllenden Gemeinden und die Gemeinden, die ihnen die Aufgaben der Verwaltungsgemeinschaft nach § 51 der ThürKO übertragen haben.

10a.7 Die Regelungen des § 29 ThürDSG hinsichtlich des Beauftragten für den Datenschutz im Rundfunk bilden im Verhältnis zu § 10a ThürDSG eine Spezialregelung. Von daher ist § 10a ThürDSG bei der Verarbeitung personenbezogener Daten durch den Rundfunk nicht anwendbar.

Zu § 11 ThürDSG

11.1 Zu den wesentlichen Funktionen des TLfD gehört es, dem Bürger als Anrufungsstelle zur Verfügung zu stehen, wenn Verletzungen des informationellen Selbstbestimmungsrechts zu besorgen sind. Die Anrufung des TLfD ist eine Sonderform des verfassungsrechtlich garantierten Petitionsrechts. Der Bürger hat Anspruch auf Tätigwerden des TLfD in angemessener Frist sowie auf Bescheidung über sein Begehren. Für die Anrufung des TLfD genügt es, wenn der Betroffene vorträgt, in seinen Belangen beeinträchtigt zu sein; er muss nicht eine bereits abgeschlossene Rechtsverletzung behaupten. Hält der TLfD aufgrund seiner durch Anrufung eingeleiteten Tätigkeit ein Einschreiten gegenüber öffentlichen Stellen für erforderlich, dann kann er mit einer Beanstandung nach § 39 ThürDSG vorgehen.

11.2 Das Benachteilungsverbot in § 11 Abs. 2 ThürDSG findet beispielsweise dann Anwendung, wenn ein Angehöriger des öffentlichen Dienstes in eigener Sache den TLfD anruft, ohne sich zuvor an seinen Dienstherrn gewandt zu haben.

11.3 Der TLfD ist nach § 11 Abs. 3 ThürDSG verpflichtet, in Fällen, in denen eine Daten verarbeitende Stelle aufgrund von § 13 Abs. 5 ThürDSG oder besonderen gesetzlichen Vorschriften dem Betroffenen keine Auskunft erteilt, in seiner Mitteilung gegenüber dem Betroffenen keine Angaben zu machen, die Rückschlüsse auf den Erkenntnisstand der Daten verarbeitenden Stelle zulassen, sofern diese einer solchen Auskunft nicht zugestimmt hat.

Zu § 12 ThürDSG

aufgehoben

Zu § 13 ThürDSG

13.1 Voraussetzung für Betroffene, ihr Recht auf informationelle Selbstbestimmung geltend zu machen, ist u.a. der Auskunftsanspruch (§ 5 Abs. 1 Nr. 3 i.V.m. § 13

ThürDSG). Hierbei hat die Daten verarbeitende Stelle (bei Auftragsdatenverarbeitung die Stelle, in deren Auftrag die Daten verarbeitet werden) entsprechend § 13 Abs. 1 ThürDSG Auskunft zu erteilen. Soweit keine (gesetzlichen) Gründe entgegen stehen, kann insbesondere aus praktischen Erwägungen oder auf Antrag des Betroffenen statt einer Auskunftserteilung auch eine Einsichtnahme in die entsprechenden Unterlagen erfolgen. Gehen Auskunftsersuchen im Rahmen einer Auftragsdatenverarbeitung bei Auftragnehmern ein, so sind diese an den Auftraggeber weiterzuleiten. Der Auskunftsanspruch richtet sich somit gegen die Daten verarbeitende Stelle bzw. gegen die für die Verarbeitung verantwortliche Stelle und bezieht sich auf alle gespeicherten Daten des Betroffenen sowie über den Zweck und die Rechtsgrundlagen der Verarbeitung. Die Herkunft der Daten und deren Empfänger sind dem Betroffenen nur mitzuteilen, soweit diese Angaben gespeichert sind; eine Speicherung dieser Daten nur für die Auskunftserteilung ist nicht erforderlich. Dem Betroffenen sind auch die Stellen mitzuteilen, denen Daten im Rahmen regelmäßiger Datenübermittlungen übermittelt werden.

13.2 Auskünfte und Akteneinsicht sind für den Betroffenen nach § 13 Abs. 2 ThürDSG in der Regel unentgeltlich, es sei denn, dass damit ein erheblicher Zeitaufwand verbunden ist. Dies kann z. B. dann der Fall sein, wenn das Auskunftsbegehren aufwändiges Suchen in Registraturen oder (bereits archivierten) Akten zur Folge hat. Dann werden für Auskünfte und Akteneinsicht Kosten gem. Thüringer Verwaltungskostengesetz i.V.m. den Maßgaben der Thüringer Allgemeinen Verwaltungkostenordnung (aktuell vom 03.12.2001, GVBl. S. 456) erhoben. Der Betroffene sollte vor der Auskunftserteilung auf die hierfür nach § 13 ThürDSG ggf. anfallenden Kosten hingewiesen werden. Entsprechendes gilt für die Erstellung von Abschriften bzw. Kopien (kostenpflichtig).
Bei Auskünften aus aktuellen, vorliegenden Unterlagen und Dateien hingegen werden in der Regel keine Kosten zu erheben sein, soweit es sich nicht um umfangreiche Unterlagen und Sachverhalte handelt.

13.3 § 13 Abs. 3 ThürDSG trifft Aussagen zu erforderlichen formellen Voraussetzungen. Der Antrag auf Auskunftserteilung ist an keine bestimmte Form gebunden, so dass sowohl schriftliche als auch mündliche Anträge entsprechend bearbeitet werden müssen. Inhaltlich soll im Antrag die Art der personenbezogenen Daten näher bezeichnet werden, über die Auskunft erteilt werden soll. Die um Auskunft ersuchte Stelle hat die Identität und Berechtigung des Antragstellers zu prüfen. Die Auskunft darf nur erteilt werden, wenn feststeht, dass der Auskunftssuchende auch mit dem Betroffenen, über den Auskunft erteilt wird, identisch ist. Telefonische Auskünfte sind daher in der Regel nicht zulässig.

Sind in Unterlagen personenbezogene Daten mehrerer Personen miteinander verbunden, müssen die Daten Dritter vor einer Einsichtnahme unkenntlich gemacht werden.

13.4 Der Auskunftsanspruch kann nach § 13 Abs. 4 und 5 ThürDSG beschränkt werden; insbesondere sind berechtigte Interessen Dritter zu berücksichtigen. Das Interesse von Behördenbediensteten gegen ein Bekanntwerden ihrer dienstlichen Tätigkeit (z. B. in Form von Stellungnahmen, Gutachten) ist nicht als „berechtigtes“ Interesse in diesem Sinne anzusehen und steht einer Auskunft daher nicht entgegen.

Entsprechendes gilt auch für die dienstliche und gesellschaftliche Tätigkeit der Beschäftigten und Funktionsträger ehemaliger Einrichtungen nach § 30 ThürDSG.

Zu § 14 ThürDSG

14.1 Stellt eine Behörde von Amts wegen fest, dass gespeicherte personenbezogene Daten unrichtig sind, so sind diese zu berichtigen. Die Unrichtigkeit gespeicherter personenbezogener Daten kann darauf beruhen, dass Daten von Anfang an falsch waren (z. B. unrichtiges Geburtsdatum) oder sich nachträglich geändert haben (z. B. Änderung des Familienstandes). Bei Daten in Akten erfolgt die Berichtigung durch einen entsprechenden Vermerk in den Akten.

14.2 Bestreitet ein Betroffener die Richtigkeit gespeicherter Daten, so hat die Behörde von Amts wegen zu ermitteln. Dabei sind drei Fälle zu unterscheiden:

- Stellt die Behörde fest, dass die gespeicherten Daten richtig sind, so bleiben die Daten gespeichert; die Tatsache, dass der Betroffene die Richtigkeit bestritten hat, ist in der Akte zu vermerken (§ 14 Satz 2 ThürDSG).
- Lässt sich weder die Richtigkeit noch die Unrichtigkeit feststellen, so sind personenbezogene Daten, die in Dateien gespeichert sind (§ 3 Abs. 7 ThürDSG) zu sperren (§ 15 Abs. 1 Nr. 2 ThürDSG). Sind die Daten in Akten gespeichert, so ist ein Vermerk in der Akte anzubringen (§ 14 Satz 2 ThürDSG).
- Wird festgestellt, dass personenbezogene Daten unrichtig sind, so ist nach Ziff. 14.1 zu verfahren. Der Betroffene kann in diesem Fall die Löschung der Daten verlangen.

Zu § 15 ThürDSG

15.1 Hinsichtlich der Verpflichtung zur Sperrung unterscheidet das Gesetz zwischen personenbezogenen Daten in Dateien (§ 15 Abs. 1 ThürDSG) und personenbezogenen Daten in Akten (§ 15 Abs. 2 ThürDSG).

15.2 Die Sperrung einzelner personenbezogener Daten in Akten wird im Hinblick auf die Besonderheiten im Aktenbereich (Vielzahl von Akten und der darin enthaltenen, zur Aufgabenerfüllung teilweise nicht mehr erforderlichen Daten) nur für Fälle angeordnet, in denen die Daten verarbeitende Stelle im Einzelfall feststellt, dass die Daten unzulässig gespeichert oder zur Aufgabenerfüllung nicht mehr erforderlich sind und ohne die Sperrung schutzwürdige Belange des Betroffenen beeinträchtigt wurden. Gleiches gilt für Daten, deren Löschung aus den in § 16 Abs. 4 ThürDSG genannten Gründen unterblieben ist.

15.3 Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur unter den einschränkenden Voraussetzungen des § 15 Abs. 3 ThürDSG übermittelt und genutzt werden.

Zu § 16 ThürDSG

16.1 Bei der Entscheidung darüber, ob Daten zur Aufgabenerfüllung der Daten verarbeitenden Stelle „noch erforderlich sind“ ist zu berücksichtigen, dass die öffentliche Verwaltung verpflichtet ist, Verwaltungsvorgänge zum Zwecke des Nachweises hoheitlichen Handelns (insbesondere bei Status begründenden Entscheidungen)

verfügbar zu halten. Gleiches gilt für die Vorhaltung von Verwaltungsvorgängen zum Zwecke der Kontrolle durch die Rechts- und Fachaufsichtsbehörden, die Gerichte, den Rechnungshof sowie den Landtag. Der Begriff der Aufgabenerfüllung umfasst daher nicht nur die Daten, die zur aktuellen Erledigung der Verwaltungsaufgabe erforderlich sind, sondern ist einschließlich der genannten Dokumentationspflichten zu verstehen. Soweit keine gesetzlichen Aufbewahrungsfristen vorgegeben sind, hat die öffentliche Stelle für die gespeicherten Daten konkrete Aufbewahrungsfristen festzulegen. Die Voraussetzungen für eine Löschung gelten gleichermaßen für in Dateien und Akten gespeicherte personenbezogene Daten, wobei eine Erforderlichkeit für die Mehrfachaufbewahrung (in Dateien und Akten) zu prüfen ist.

16.2 In Akten gespeicherte personenbezogene Daten sind im Falle des § 16 Abs. 1 Nr. 2 ThürDSG erst dann zu löschen, wenn die gesamte Akte zur Aufgabenerfüllung nicht mehr erforderlich ist. Bis zu diesem Zeitpunkt sind die Daten, deren Kenntnis zur Erfüllung der Aufgabe nicht mehr erforderlich ist, zu sperren.
Unzulässig gespeicherte Daten sind dagegen zu löschen.

16.3 Die Verpflichtung zur Löschung darf nicht dazu führen, dass die Überlieferung historisch bedeutsamer Vorgänge an die Nachwelt unmöglich gemacht wird. Vor der Löschung/Vernichtung nicht mehr benötigter Daten und Unterlagen sind diese dem zuständigen Archiv (§ 11 ThürArchivG) zur Übernahme anzubieten. Es empfiehlt sich, mit dem zuständigen Archiv über den Einzelfall hinausgehende Regelungen zur Feststellung der Archivwürdigkeit bzw. zur Übernahme von Daten zu treffen. Ist aufgrund spezialgesetzlicher Normen eine Löschung vorgesehen (beispielsweise bei Disziplinarvorgängen), sind entsprechende Abstimmungen mit dem zuständigen Archiv erforderlich. Unzulässig gespeicherte Daten sind von der Verpflichtung, sie vor Löschung dem Archiv anzubieten, ausgenommen.

16.4 § 16 Abs. 4 ThürDSG regelt die Fälle, in denen eine Löschung ausnahmsweise unterbleibt. An die Stelle der Löschung tritt nach § 15 Abs. 1 Nr. 2 ThürDSG in diesen Fällen die Sperrung.

16.5 Absatz 5 stellt klar, dass nach Wegfall der in Absatz 4 genannten Gründe, die nach § 15 Abs. 1 Nr. 2 ThürDSG gesperrten Daten endgültig zu löschen sind.

Zu § 17 ThürDSG

Die Benachrichtigung regelmäßiger Datenempfänger von einer Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung dient dem Schutz des Bürgers und enthebt ihn der Mühe, seine entsprechenden Ansprüche bei allen Datenempfängern zu erheben. Die Benachrichtigung anderer Stellen hat jedoch nur zu erfolgen, soweit dies im Interesse des Betroffenen erforderlich erscheint.

Zu § 18 ThürDSG

Nach Artikel 23 EG-Datenschutzrichtlinie kann jeder, dem durch rechtswidrige Datenverarbeitung ein Schaden entstanden ist, von der verantwortlichen Stelle Schadenersatz verlangen. Die Richtlinie begründet damit eine Haftung für vermutetes Verschulden mit gleichzeitiger Entlastungsmöglichkeit. Absatz 1 übernimmt die Regelung zur Verschuldenshaftung; öffentliche Stellen haften nicht, wenn sie den

Nachweis führen, dass die gebotene Sorgfalt beachtet wurde und sie demzufolge kein Verschulden trifft. Die Schadensersatzregelung differenziert dabei nicht danach, ob der Schaden durch unzulässige/unrichtige automatisierte oder nicht automatisierte Datenverarbeitung entsteht.

Der Betroffene ist nicht auf den Schadensersatzanspruch des § 18 ThürDSG beschränkt, sondern kann seinen Anspruch alternativ auch auf andere Rechtsgrundlagen stützen.

Zu § 19 ThürDSG

19.1 Personenbezogene Daten dürfen nur erhoben werden, wenn ihre Kenntnis zur Erfüllung der Aufgabe der erhebenden Stelle erforderlich ist. Dies ist dann der Fall, wenn die Daten zur Aufgabenerfüllung objektiv geeignet sind und die Erhebung im Hinblick zum angestrebten Verwendungszweck verhältnismäßig ist. Zum Begriff der „Erhebung“ vgl. Ziff. 3.3.1. Vor einer Erhebung personenbezogener Daten sollte jedoch stets geprüft werden, ob die Aufgaben auch mit anonymisierten oder pseudonymisierten Daten erfüllt werden können.

19.2 § 19 ThürDSG legt die Voraussetzungen fest, unter denen eine öffentliche Stelle Daten erheben darf. Ob der erhebenden Stelle von einer anderen öffentlichen oder privaten Stelle die Daten übermittelt werden dürfen, bestimmt sich nach den für die übermittelnde Stelle geltenden Vorschriften über die Datenübermittlung, bei einer Nutzung für einen anderen Zweck durch Weitergabe innerhalb derselben Stelle ist § 20 ThürDSG zu beachten. Die bloße Zulässigkeit der Erhebung allein gibt einer Stelle also keine rechtliche Möglichkeit oder gar einen Anspruch darauf, die Daten von einer anderen Stelle zu erhalten. Ist eine Datenübermittlung erlaubt (z. B. nach § 21 ThürDSG), so ist auch die Erhebung durch den Empfänger zulässig (§ 19 Abs. 2 Satz 1 Nr. 1 ThürDSG). Vorab ist allerdings zu prüfen, ob die Daten beim Betroffenen zu erheben sind.

19.3 Werden personenbezogene Daten beim Betroffenen mit seiner Kenntnis erhoben (z. B. auf Vordrucken), so ist der Erhebungszweck ihm gegenüber anzugeben. Ist der Betroffene aufgrund einer Rechtsvorschrift zur Auskunft verpflichtet oder ist die Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben, hinzuweisen.
Beispiele:

a) wenn der Betroffene aufgrund einer Rechtsvorschrift zur Angabe verpflichtet ist: „Hinweis nach § 19 Abs. 3 des Thüringer Datenschutzgesetzes: Rechtsgrundlage für die Erhebung dieser Daten ist ... (Angabe der betreffenden Rechtsnorm mit Artikel- oder §§-Angabe). Die Daten werden an ... übermittelt (Angabe der betreffenden Rechtsnorm mit Artikel- oder Paragraphenangabe).“;

b) wenn die Daten zur Bearbeitung eines Antrages des Betroffenen erforderlich sind: „Hinweis nach § 19 Abs. 3 des Thüringer Datenschutzgesetzes: Die Angaben sind erforderlich, um zu prüfen, ob die Voraussetzungen für ... vorliegen. Rechtsgrundlage ist ... (Angabe der betreffenden Rechtsnorm mit Artikel- oder §§-Angabe). Die Daten werden an ... übermittelt (Angabe der betreffenden Rechtsnorm mit Artikel- oder Paragraphenangabe).“;

c) wenn keine Rechtsvorschrift den Betroffenen zur Angabe verpflichtet und die Daten nicht zur Bearbeitung eines Antrages des Betroffenen erforderlich sind: „Hinweis nach § 19 Abs. 3 des Thüringer Datenschutzgesetzes: Die Angaben (in Nummer ... dieses Vordrucks) sind freiwillig. Sie werden benötigt, um ... Die Daten werden an ... übermittelt. Sie können von diesen Angaben absehen, ohne Rechtsnachteile befürchten zu müssen.“.

Zu § 20 ThürDSG

20.1 Zum Begriff „erforderlich“ wird auf Ziff. 19.1 verwiesen. § 20 Abs. 1 ThürDSG verankert das Prinzip der Zweckbindung: Personenbezogene Daten dürfen nur für Zwecke gespeichert, verändert oder genutzt werden, für die sie erhoben worden sind. Zweck einer Erhebung ist nicht nur die Bearbeitung eines Einzelfalls, für den die Daten erforderlich sind; maßgeblich ist vielmehr der gesetzlich bestimmte Zweck, zu deren Erfüllung die Daten erhoben werden (z. B. Vollzug baurechtlicher Vorschriften, Vollzug gewerberechtlicher Vorschriften). Bei der Prüfung, ob der gleiche Zweck vorliegt, ist daher entscheidend, für welche gesetzlich normierte Verwaltungsaufgabe die Daten erhoben worden sind, nicht aber darauf, aus welchem Anlass dies geschehen ist. Geht einer Veränderung oder Nutzung keine Erhebung voraus, so gilt dies für den Zweck der Speicherung entsprechend. Erfolgt die Erhebung von Daten aufgrund einer Einwilligung des Betroffenen, so ist die Speicherung, Veränderung oder Nutzung nur soweit zulässig, wie der Betroffene wirksam eingewilligt hat.

20.2 In § 20 Abs. 2 ThürDSG werden abschließend die Fälle aufgezählt, in denen vom Gebot der Zweckbindung abgewichen werden darf.

20.3 § 20 Abs. 3 ThürDSG ordnet eine Reihe von Nebenzwecken dem Hauptzweck zu. Dies ermöglicht es, dass für die öffentliche Verwaltung unentbehrliche Aufsichts- und Kontrollbefugnisse und die übrigen genannten Tätigkeiten wahrgenommen werden können.

20.4 Zur Datenschutzkontrolle und Datensicherung gehört im weitesten Sinn auch die dienst-, arbeits-, haftungs- und strafrechtliche Ahndung von datenschutzrechtlichen Verstößen; diesbezügliche Maßnahmen werden durch die Zweckbindung nicht behindert.

Zu § 21 ThürDSG

§ 21 ThürDSG regelt lediglich die Befugnis (Zulässigkeit) der Datenübermittlung; eine Verpflichtung kann sich insbesondere aus der Amtshilfepflicht nach den Bestimmungen des Thüringer Verwaltungsverfahrensrechts ergeben. Amtshilfe durch Übermittlung von Daten wird auch Informationshilfe genannt. Auch die Informationshilfe durch Datenübermittlung setzt voraus, dass die Datenübermittlung mit dem Datenschutzrecht vereinbar ist. Ist eine Datenübermittlung nach § 21 ThürDSG oder nach den dafür geltenden bereichsspezifischen Vorschriften zulässig, so ist eine um Übermittlung ersuchte öffentliche Stelle nach den Grundsätzen und in den Grenzen der Amtshilfe zur Übermittlung an die ersuchende Stelle auch verpflichtet.

Öffentliche Stelle im Sinne von § 21 ThürDSG sind abweichend von § 2 Abs. 1 und 2 ThürDSG auch die entsprechenden Stellen des Bundes oder der anderen Bundes

länder. Die Weitergabe von Daten an den Betroffenen sowie zwischen Auftraggeber und Auftragnehmer stellt keine Datenübermittlung nach § 21 ThürDSG dar.

§ 21 Abs. 1 ThürDSG knüpft die Zulässigkeit einer Datenübermittlung zwischen öffentlichen Stellen an zwei Voraussetzungen. Zum einen muss die Übermittlung zur Erfüllung der Aufgaben der übermittelnden Stelle oder des Empfängers erforderlich sein (vgl. Ziff. 19.1). Zum anderen muss die Zweckbindung entsprechend der Vorschriften des § 20 ThürDSG beachtet werden. Für Datenübermittlungen zwischen öffentlichen Stellen ist der Grundsatz der Zweckbindung also ebenso zu beachten wie bei einer Datennutzung innerhalb einer öffentlichen Stelle (siehe hierzu auch Ausführungen im letzten Absatz).

Bei der Übermittlung personenbezogener Daten sieht § 21 Abs. 4 ThürDSG eine Ausnahme vom Erforderlichkeits- und Zweckbindungsgrundsatz in Bezug auf verbundene Daten in Akten dann vor, wenn die Daten nur deshalb übermittelt werden (müssen), weil sie von den eigentlich zu verarbeitenden Daten nicht oder nur mit unvertretbarem Aufwand abzutrennen sind. Die Übermittlung ist nur nach Maßgabe einer Interessenabwägung zulässig. Eine Nutzung der Überschussinformationen durch den Empfänger ist unzulässig.

Für die Weitergabe personenbezogener Daten innerhalb der Daten verarbeitenden Stelle gelten die gleichen Anforderungen wie für Übermittlungen an Dritte. Soweit innerhalb der Daten verarbeitenden Stelle ein automatisiertes Abrufverfahren eingerichtet ist, sind die besonderen Zulässigkeitsanforderungen des § 7 Abs. 6 ThürDSG zu beachten.

Zu § 22 ThürDSG

22.1 § 22 Abs. 1 ThürDSG begründet keinen Anspruch eines privaten Dritten auf Übermittlung personenbezogener Daten. Wenn sich ein solcher Anspruch nicht aus anderen Vorschriften ergibt, steht eine solche Auskunftserteilung im pflichtgemäßen Ermessen der Daten verarbeitenden Stelle, soweit die in § 22 Abs. 1 ThürDSG genannten Zulässigkeitsvoraussetzungen vorliegen.

22.2 Bei der Übermittlung nach § 22 Abs. 1 Nr. 2 ThürDSG ist in jedem Einzelfall von der Daten verarbeitenden Stelle zu prüfen, ob der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft dargelegt hat und ob der Betroffene ein schutzwürdiges Interesse am Ausschluß der Übermittlung hat. Hierbei sind unter anderem die Art der zu übermittelnden Daten, ihr Verwendungszweck beim Empfänger sowie ein etwaiger der abgebenden Stelle bekanntgewordener entgegenstehender Wille des Betroffenen in die Abwägung einzubeziehen. Zu den berechtigten Interessen des Empfängers gehört jedes von der Rechtsordnung als schutzwürdig anerkannte ideelle oder vermögenswerte Interesse, auch ein wirtschaftliches Interesse.

Bei der Abwägung ist davon auszugehen, dass es im Regelfall nicht Aufgabe öffentlicher Stellen ist, die von ihnen zur Erfüllung ihrer Aufgaben gespeicherten Daten Betroffener an Private zu übermitteln.

Auskünfte, die der Private aus den Melderegistern erhalten kann, werden von

anderen öffentlichen Stellen im Regelfall nicht erteilt.

22.3 Die Benachrichtigung des Betroffenen nach § 22 Abs. 1 Nr. 2 ThürDSG unterbleibt, wenn er von der Übermittlung bereits Kenntnis erlangt hat oder erlangen wird, etwa weil er vom Empfänger der Daten unterrichtet wird. Von der Benachrichtigung kann auch abgesehen werden, wenn es sich z. B. um wenig sensible Daten handelt, die üblicherweise bekanntgegeben werden (z. B. Name, Funktion und Dienstanschrift von Mandatsträgern).

22.4 Auskünfte über mehrere vom Empfänger nicht namentlich bezeichnete Personen (Gruppenauskünfte) sollen nur erteilt werden, wenn sie im öffentlichen Interesse liegen. Fehlt ein öffentliches Interesse, darf Auskunft nur erteilt werden, wenn die Betroffenen zugestimmt haben. Da die Zustimmung der Betroffenen häufig nur mit besonderen Schwierigkeiten eingeholt werden kann, kommt in Fällen, in denen z. B. Forschungseinrichtungen, Meinungsforschungsinstitute oder auch ehemalige Schulfreunde Adressdaten einer abgegrenzten Personengruppe erhalten wollen, um mit diesen in Kontakt zu treten, das sog. Adressmittlungsverfahren in Betracht. Dabei erstellen die Auskunftsbegehrenden Anschreiben (in ausreichender Anzahl), in denen ihr Anliegen und der Wunsch zur Kontaktaufnahme enthalten ist. Diese werden der Daten verarbeitenden Stelle übergeben, die auf die Umschläge die Adressaufkleber aufbringt und diese gegen Kostenerstattung versendet. Auf diese Weise können die Auskunftsbegehrenden Kontakt mit den Betroffenen aufnehmen, ohne dass ihnen die Adressdaten bekannt werden. Im Anschreiben sollte auf diese Verfahrensweise hingewiesen werden, um Zweifel bei den Betroffenen nicht entstehen zu lassen, dass die Daten verarbeitende Stelle die Adressdaten übermittelt hat. Ein Rechtsanspruch auf Durchführung des Adressmittlungsverfahrens besteht ebenso wie auf eine Datenübermittlung nicht.

22.5 Die Datenübermittlung an Private - einschließlich der Frage der Benachrichtigung des Betroffenen - ist in vielen Bereichen spezialgesetzlich geregelt. Dies gilt beispielsweise für die Einsichtnahme in viele öffentliche Register (z. B. Grundbuch, Schuldnerverzeichnis).

Zu § 23 ThürDSG

23.1 § 23 Abs. 1 ThürDSG trägt dem Umstand Rechnung, dass nach Umsetzung der EG Datenschutzrichtlinie in deren Geltungsbereich die Übermittlung personenbezogener Daten nicht von strengeren Voraussetzungen abhängig gemacht werden darf als im Inland, um den gemäß Artikel 1 Abs. 2 der EG Datenschutzrichtlinie garantierten freien Datenverkehr nicht zu behindern.

Für die Übermittlung an Stellen außerhalb der Europäischen Union gelten wie bisher regelmäßig die gleichen Grundsätze wie für Übermittlungen an nicht öffentliche Stellen. Es wird nicht danach unterschieden, ob die Stelle, der Daten übermittelt werden, eine öffentliche oder nicht öffentliche Stelle ist.

Bei der Stelle, der Daten übermittelt werden, muss ein angemessenes Datenschutzniveau bestehen. Die Regelung lehnt sich insoweit an § 4b Abs. 2 BDSG an. Ein angemessenes Datenschutzniveau ist gegeben, wenn unter Berücksichtigung aller Umstände, die bei der Übermittlung bedeutsam sind, wie der Art der Daten, der

Zweckbestimmung und der im Empfängerland geltenden Rechtsvorschriften, Standesregeln und Sicherheitsmaßnahmen ein dem innereuropäischen Standard gleichwertiger Schutz personenbezogener Daten gegeben ist.

Die Angemessenheit als Voraussetzung der Übermittlung in Drittstaaten muss zunächst von der übermittelnden Stelle selbst geprüft werden. Die Angemessenheit oder ihr Fehlen können aber auch in einem von der EG Datenschutzrichtlinie festgelegten Verfahren durch die Europäische Kommission festgestellt werden. Die Mitgliedsstaaten haben dann die aufgrund der Feststellungen gebotenen Maßnahmen zu treffen; das heißt, sie haben dafür zu sorgen, dass beim Fehlen des Niveaus keine Datenübermittlungen in diese Länder stattfinden. Auf die Einhaltung der Zweckbindung ist bei der Übermittlung ins Ausland zu achten.

23.2 § 23 Abs. 2 ThürDSG regelt die Zulässigkeitsvoraussetzungen in Umsetzung des Artikel 26 der EG Datenschutzrichtlinie für den Fall, dass ein Drittstaat kein angemessenes Schutzniveau im Sinne von Absatz 1 aufweist, jedoch eine Übermittlung dorthin erforderlich ist.

Zu § 24 ThürDSG

Durch § 24 ThürDSG werden personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis (vgl. Ziff. 7.1) unterliegen und die der Daten verarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person oder Stelle in Ausübung der Berufs- oder Amtspflicht zur Verfügung gestellt worden sind, einer strengen, weitergehenden Zweckbindung unterworfen. Damit soll erreicht werden, dass die besonderen Zweckbindungen solcher Daten auch nach einer Weitergabe an eine Stelle beachtet werden, die keinem Berufs- oder besonderem Amtsgeheimnis unterliegt und die ohne die Regelungen des § 24 ThürDSG nach den §§ 20-22 ThürDSG Zweckänderungen vornehmen könnte. Durch den Begriff „zur Verfügung gestellt worden“ wird deutlich, dass es sich sowohl um Daten handelt, die von einem Berufsgeheimnisträger der Daten verarbeitenden Stelle übermittelt worden sind als auch um solche Daten, die innerhalb einer Daten verarbeitenden Stelle (z. B. vom Gesundheitsamt an die Ausländerbehörde) weitergegeben wurden, was aufgrund des organisatorischen Behördenbegriffs (vgl. 2.1) keine Übermittlung sondern eine Nutzung darstellt. Die Verarbeitung oder Nutzung für andere Zwecke wird in Absatz 1 grundsätzlich ausgeschlossen. Nach Absatz 2 ist eine Zweckänderung nur durch Zulassung in einem besonderen Gesetz (also nicht dem ThürDSG) erlaubt. Eine Zweckänderung ist auch mit Einwilligung des Betroffenen möglich, ohne dass dies ausdrücklich erwähnt zu werden braucht.

Weitere besondere Amtsgeheimnisse bestehen z. B. nach § 30 Abgabenordnung (Steuergeheimnis), § 35 SGB I (Sozialgeheimnis) und § 16 Bundesstatistikgesetz (Statistikgeheimnis).

Zu § 25 ThürDSG

25.1 § 25 ThürDSG regelt entsprechend dem Anwendungsbereich des ThürDSG lediglich die Datenverarbeitung durch öffentliche Forschungseinrichtungen (vgl. Ziff. 2.1 ff.). Die an anderen Stellen des Gesetzes getroffenen Regelungen zur Verarbeitung personenbezogener Daten zu Forschungszwecken bleiben unberührt (vgl. § 20

Abs. 2 Nr. 9 i.V.m. § 21 Abs. 1 Nr. 2 und § 22 Abs. 1 Nr. 1, § 15 Abs. 3 Nr. 1 ThürDSG). Dies gilt insbesondere auch für die Datenübermittlung durch öffentliche Stellen an Forschungseinrichtungen. Auf die Regelung über die Einwilligung in die Verarbeitung personenbezogener Daten in § 4 Abs. 4 ThürDSG wird hingewiesen.

25.2 § 25 Abs. 1 ThürDSG schließt die Verarbeitung der zu wissenschaftlichen Zwecken erhobenen oder erstmals gespeicherten Daten für andere als wissenschaftliche Zwecke aus und enthält damit eine besondere Zweckbindungsregelung, mit der sichergestellt werden soll, dass solche Daten im Bereich der wissenschaftlichen Verwendung verbleiben. Die in § 20 Abs. 2 ThürDSG enthaltenen Ausnahmen von der Zweckbindung finden hier keine Anwendung. Personenbezogene Daten, die für Zwecke der wissenschaftlichen Forschung erhoben worden sind, können über das ursprüngliche Vorhaben hinaus auch für andere Forschungsvorhaben verwendet werden. Dies schließt die Übermittlung an Forschungseinrichtungen mit ein, die andere Forschungsaufgaben haben. Soweit die Verarbeitung der Daten durch die Forschungseinrichtung auf einer Einwilligung des Betroffenen beruht, dürfen die Daten für Zwecke der wissenschaftlichen Forschung nur in dem Umfang verarbeitet werden, wie dies durch die Einwilligung gedeckt ist.

25.3 Der Begriff der Anonymisierung ist in § 3 Abs. 9 ThürDSG definiert. Bis zur Anonymisierung sind die Hilfsmerkmale von den Erhebungsmerkmalen gesondert zu speichern.

Zu § 26 ThürDSG

26.1 Öffentliche Stellen nehmen am Wettbewerb teil, wenn sie Leistungen erbringen, die auch von Privaten erbracht werden können und sie keine Monopolstellung einnehmen. Kein Wettbewerb liegt vor, wenn ein Anschluss- oder Benutzungszwang für eine öffentliche Einrichtung besteht oder wenn öffentliche Stellen hoheitlich handeln (z. B. Zwangseinweisung durch Krankenhäuser). Als öffentliche Stellen, die am Wettbewerb teilnehmen, gelten beispielsweise Unternehmen, die öffentlich-rechtlich organisiert sind (z. B. Eigenbetriebe od. selbstständige Anstalten des öffentlichen Rechts), Sparkassen, Krankenhäuser in öffentlich-rechtlicher Trägerschaft, öffentlich-rechtliche Kreditinstitute und Versicherungsanstalten.

26.2 Öffentliche Stellen, die am Wettbewerb teilnehmen, unterliegen uneingeschränkt der Kontrolle des TLfD. Für den Umgang mit personenbezogenen Daten gelten die Vorschriften des BDSG bzw. bereichsspezifische Vorschriften (z. B. Thüringer Krankenhausgesetz), ansonsten das ThürDSG. In der Frage der Anwendbarkeit des BDSG oder des ThürDSG ist - soweit öffentliche Stellen zugleich als Wettbewerbsunternehmen tätig werden - maßgeblich darauf abzustellen, in welchem Bereich der Schwerpunkt der Datenverarbeitung oder -nutzung liegt.

Zu § 27 ThürDSG

27.1 Von ausreichenden Datenschutzmaßnahmen bei den öffentlich-rechtlichen Religionsgesellschaften ist dann auszugehen, wenn sie den im staatlichen Bereich für vergleichbare Daten getroffenen Datenschutzmaßnahmen entsprechen.

27.2 Bei den Religionsgemeinschaften handelt es sich um Körperschaften des öffentlichen Rechts, die nicht der Aufsicht des Landes unterstehen und deshalb nach § 2 Abs. 1 vom Anwendungsbereich des ThürDSG ausgenommen sind. Im Bereich der katholischen und evangelischen Kirche gelten eigene Datenschutzregelungen, die im Wesentlichen denen für öffentliche Stellen entsprechen. Darüber hinaus kann das Thüringer Innenministerium im Einvernehmen mit dem Thüringer Kultusministerium auf Antrag feststellen, ob eine Stelle als öffentlich-rechtliche Religionsgesellschaft im Sinne des § 27 ThürDSG anzusehen ist und ob bei dieser Stelle ausreichende Datenschutzmaßnahmen getroffen sind.

Zu § 28 ThürDSG

Im Interesse der Presse- und Rundfunkfreiheit (Artikel 5 Grundgesetz) werden in § 28 ThürDSG Ausnahmen vom Anwendungsbereich des ThürDSG für die journalistisch-redaktionelle Tätigkeit des öffentlich-rechtlichen Rundfunks geschaffen. Außerhalb des Bereichs der journalistisch-redaktionellen Tätigkeit gelten die Vorschriften des ThürDSG für die Rundfunkanstalten. Sie unterliegen jedoch nicht der Kontrolle des TLfD, sondern nach § 29 ThürDSG der des Beauftragten für den Datenschutz im Rundfunk.

Eine Gegendarstellung des Betroffenen (§ 28 Abs. 2 ThürDSG) ist zusammen mit dem gesendeten Material aufzubewahren. Der Anspruch auf Auskunft besteht erst dann, wenn die Berichterstattung erfolgt ist. Das Auskunftsverweigerungsrecht des § 28 Abs. 3 Satz 2 ThürDSG trägt dem Informationsschutz Rechnung (vgl. dazu das Zeugnisverweigerungsrecht in § 53 Abs. 1 Nr. 5 Strafprozeßordnung). § 28 Abs. 3 Satz 3 ThürDSG stellt klar, dass ein Berichtigungsanspruch in jedem Fall zu erfüllen ist.

Zu §§ 30 bis 33 ThürDSG

In den §§ 30 bis 33 ThürDSG wird der Umgang mit personenbezogenen Daten aus ehemaligen staatlichen oder wirtschaftsleitenden Organen, Kombinaten, Betrieben oder sonstigen Einrichtungen sowie gesellschaftlichen Organisationen der DDR geregelt, soweit diese nicht zwischenzeitlich rechtmäßig von öffentlichen Stellen übernommen bzw. gespeichert sind. Eine beispielhafte Aufzählung ehemaliger staatlicher oder wirtschaftsleitender Organe, Kombinate, Betriebe oder Einrichtungen sowie gesellschaftlicher Organisationen der Deutschen Demokratischen Republik ist der Anlage 2 der Hinweise zum ThürDSG zu entnehmen.

Zu § 34 ThürDSG

34.1 Diese Vorschrift weist die Verantwortung für den Vollzug datenschutzrechtlicher Vorschriften den Landesministerien, den Gemeinden und Gemeindeverbänden sowie den sonstigen der Aufsicht des Landes unterstehenden Organisationseinheiten zu. Adressaten der Datenschutzvorschriften sind die jeweiligen Leiter der Daten verarbeitenden Stellen. Eine Delegation der Pflichten auf den Datenschutzbeauftragten ist nicht zulässig. Zur Sicherstellung des Datenschutzes gehört neben der Einhaltung des materiellen Datenschutzrechts (ThürDSG und spezielles Bundes- und Landesrecht, Kommunale Satzungen) die Organisation des verwaltungsinternen Handelns zum Vollzug der §§ 9, 10, 10a und 34 ThürDSG.

34.2 Zweck der datenschutzrechtlichen Freigabe ist die Vorabkontrolle der Zulässigkeit der automatisierten Verarbeitung personenbezogener Daten. Die Verpflichtung zur Freigabe besteht unabhängig davon, ob ein automatisiertes Verfahren durch den Anwender selbst erstellt oder von Dritten übernommen wird. Durch geeignete organisatorische Regelungen ist sicherzustellen, dass automatisierte Verfahren erst nach der vorherigen schriftlichen Freigabe zum Einsatz gelangen. Damit werden letztlich auch Ausgaben vermieden, die durch den Einsatz von Verfahren entstehen, die infolge eines Verstoßes gegen datenschutzrechtliche Bestimmungen nicht einsetzbar sind. Ein unterlassenes Freigabeverfahren ist umgehend nachzuholen.

Als Mindestvoraussetzung für die datenschutzrechtliche Dokumentation hat der für die automatisierte Verarbeitung unmittelbar verantwortliche Leiter der Organisationseinheit das Formblatt für den Eintrag in das Verfahrensverzeichnis nach § 10 ThürDSG entsprechend der Anlage 1 der Hinweise zum ThürDSG zu erstellen.

Einzelheiten zum Verfahren können die in § 34 Abs. 1 ThürDSG genannten Normadressaten für ihren Bereich durch Erlass regeln. Für den Bereich der Ministerialverwaltung empfiehlt sich folgende Verfahrensweise:

1. Anträge auf Freigabe sind von der Organisationseinheit, die den Einsatz des automatisierten Verfahrens beabsichtigt, unter Einhaltung des Dienstweges dem fachlich zuständigen Abteilungsleiter des Ministeriums zur Entscheidung vorzulegen. Dem Antrag sind die Formblätter zum Verfahrensverzeichnis (siehe Anlage 1 der Hinweise zum ThürDSG) sowie ein Vermerk (Muster in Anlage 3a der Hinweise zum ThürDSG), der die Beteiligung der verantwortlichen Funktionsträger und hier insbesondere die Beteiligung des für die Behörde bestellten internen Beauftragten für den Datenschutz (siehe Ziff. 10a.2) an der Vorbereitung der Entscheidung ausweist, beizufügen. Bei Anträgen aus dem nachgeordneten Bereich kann – ergänzend zur Beteiligung des jeweiligen behördeninternen Beauftragten für den Datenschutz – der Beauftragte für den Datenschutz des Ministeriums beigezogen werden. Dies kann beispielsweise geboten sein, wenn dem zum Einsatz kommenden Verfahren behördenübergreifende Bedeutung zu kommt (Muster in Anlage 3b der Hinweise zum ThürDSG).

2. Die Freigabeentscheidung ist der das Verfahren betreibenden Organisationseinheit zur Kenntnis zu geben, der Beauftragte für den Datenschutz erhält die Formblätter zur Aufnahme in das von ihm geführte Verfahrensverzeichnis (Anlage 3c).

Die Regelungen für die Freigabe von Verfahren gelten entsprechend auch bei Auftragsdatenverarbeitung nach § 8 ThürDSG (für die Freigabe hat der Auftraggeber zu sorgen) und für automatisierte Abrufverfahren (Online-Anschlüsse), die Dritten den Zugriff auf personenbezogene Daten gestatten. Nach § 7 Abs. 3 Satz 1 ThürDSG ist vor der Freigabe derartiger Abrufverfahren rechtzeitig der TLfD zu unterrichten.

34.3 Absatz 3 sieht für die dort bezeichneten Verfahren eine Pflicht zur Freigabe nicht vor, da sie im Vergleich zur eigentlichen Sachbearbeitung nur eine untergeordnete Hilfsfunktion darstellen. Diese Verfahren sind nicht oder nur eingeschränkt geeignet, das Persönlichkeitsrecht der Betroffenen zu gefährden. Die Verantwortlichen sind gehalten, das Vorliegen der genannten Ausnahmebedingungen in eigener Verantwortung zu prüfen und festzustellen. Hierbei ist nicht auf die Bezeichnung des

Verfahrens, sondern auf seine Zweckbestimmung abzustellen. Nur die Verfahren, die ausschließlich einem der genannten Zwecke dienen, sind von der Freigabe befreit. Im Zweifel ist der Beauftragte für den Datenschutz zu beteiligen.

Zu den in Nummer 1 erwähnten Verfahren zählen:

- Verfahren, die ausschließlich der Erstellung von Texten dienen und bei denen die personenbezogenen Daten gelöscht werden, sobald sie für diesen Zweck nicht mehr benötigt werden (Textverarbeitungsverfahren),
- Verfahren, die ausschließlich dem Auffinden von Vorgängen, Anträgen oder Akten dienen (Registraturverfahren),
- Verfahren zur Überwachung von Terminen und Fristen,
- Telefon-, Telefax- und sonstige Kommunikations- und Teilnehmerverzeichnisse,
- Zimmer-, Inventar- und Softwareverzeichnisse.

Die in Nummer 2 bezeichneten Verfahren sind solche, die z. B. eine Überprüfung der Übermittlung personenbezogener Daten in automatisierten Abrufverfahren durch geeignete Stichprobenverfahren ermöglichen sollen sowie solche, die die Verwaltung der Zugriffsrechte und die Protokollierung der Zugriffe beinhalten.

Bei den in Nummer 3 bezeichneten Verfahren handelt es sich z. B. um die automatisierte Führung der Grundbücher, der Handelsregister, des Registers der Datenschutzaufsicht, der Verzeichnisse beliehener Sachverständiger sowie des Verzeichnisses öffentlich bestellter Vermessungsingenieure.

Absatz 3 Satz 2 sieht für weitere Verfahren, die eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen nicht erwarten lassen, eine Freigabe dann als entbehrlich an, wenn eine Rechtsverordnung abschließend bestimmt, bei welchen Verfahren und Stellen diese Voraussetzungen gegeben sind. Diese Regelung stützt sich auf Artikel 18 Abs. 2, erster Anstrich der EG-Datenschutzrichtlinie, der einen Wegfall der Meldepflicht (hier an das beim Beauftragten für den Datenschutz zu führende Verfahrensverzeichnis) für bestimmte Verarbeitungskategorien erlaubt. Der sonst im Rahmen des Freigabeverfahrens vorzulegende Datenkatalog ist dann schon abschließend in der Rechtsverordnung enthalten. Damit wird auch den Anforderungen des Art. 21 Abs. 3 der EG-Datenschutzrichtlinie entsprochen, wonach Verarbeitungen, die von der Meldung ausgenommen sind, in geeigneter Weise verfügbar zu machen sind.

Absatz 3 Satz 3 erlaubt den Ministerien, bei Vorliegen der genannten Voraussetzungen eine entsprechende Rechtsverordnung zu erlassen.

Wenngleich die in Absatz 3 Satz 1 Nr.3 und Satz 2 bezeichneten Verfahren keine Aufnahme in das Verfahrensverzeichnis finden, sollte gegenüber dem Beauftragten für den Datenschutz eine Mitteilung erfolgen (vgl. Ziff. 10.4).

Zu § 36 ThürDSG

Die Geschäftsstelle des TLfD kann im Einzelfall mit Zustimmung des TLfD auch zu Überwachungsaufgaben im nicht öffentlichen Bereich herangezogen werden (§ 42 Abs. 1 ThürDSG).

Zu § 37 ThürDSG

37.1 Der Kontrolle des TLfD unterliegen alle öffentlichen Stellen (§ 2 ThürDSG) einschließlich der öffentlichen Stellen, die am Wettbewerb teilnehmen.

37.2 Das Kontrollrecht des TLfD nach § 37 ThürDSG hängt nicht davon ab, ob die Daten verarbeitende Stelle die Betroffenen über das Widerspruchsrecht nach § 37 Abs. 2 Satz 3 ThürDSG unterrichtet hat. Der TLfD kann personenbezogene Daten, die dem Arztgeheimnis unterliegen, und personenbezogene Daten in Personalakten oder Akten über die Sicherheitsüberprüfung auch dann prüfen, wenn die Daten verarbeitende Stelle es versäumt hat, die Betroffenen in allgemeiner Form auf ihr Widerspruchsrecht aufmerksam zu machen. Voraussetzung für eine Kontrollbefugnis in den in § 37 Abs. 2 ThürDSG genannten Fällen ist ausschließlich das Nichtvorhandensein eines Widerspruchs durch den Betroffenen. Die Unterrichtung in allgemeiner Form nach § 37 Abs. 2 Satz 3 ThürDSG kann z. B. durch einen entsprechenden Hinweis in dem Aufnahmeantrag bei Krankenhäusern in Vordrucken u. Personalakten, Sicherheitsüberprüfungen usw. oder durch Bekanntgabe in dienstlichen Nachrichten geschehen.

Die Unterrichtungspflicht verlangt nicht, dass der Betroffene von einer unmittelbar bevorstehenden Kontrolle durch den TLfD zu unterrichten ist; dies ist allerdings auch nicht ausgeschlossen.

In der Unterrichtung ist auf die Kontrollbefugnis des TLfD (§ 37 Abs. 1 Abs. 2 Satz 1 und Satz 2 ThürDSG) und auf dessen Verschwiegenheitspflicht hinzuweisen.

Der Widerspruch nach § 37 Abs. 2 Satz 2 ThürDSG ist höchstpersönlich und unterbindet daher nur die Datenschutzkontrolle in Bezug auf die Daten des Widersprechenden selbst. Der Widerspruch ist unmittelbar bei den Daten des Betroffenen zu speichern, auf die er sich bezieht. Dem TLfD ist der Widerspruch auf Verlangen vorzulegen.

Zu § 38 ThürDSG

38.1 Die der Kontrolle unterstehenden Behörden und Stellen sind allgemein und umfassend zur Unterstützung des TLfD und seiner Beauftragten verpflichtet. Die Unterstützung soll eine effektive Kontrolle im Interesse des Schutzes des betroffenen Bürgers ermöglichen. Verlangt der TLfD Unterstützung, so kann die Behörde oder Stelle nicht unter Hinweis auf ihre sonstigen Verpflichtungen untätig bleiben.

38.2 Verlangt der TLfD Einsicht in Unterlagen und Akten, so ist sie zu gewähren, wenn ein Zusammenhang mit der Kontrolle besteht. Für den geforderten Zusammenhang genügt es, dass die Akten oder Unterlagen nach Lage der Dinge möglicherweise etwas darüber aussagen, ob, wann und wie die Daten verarbeitende Stelle den Anforderungen des Datenschutzes nachgekommen ist.
Dazu gehören u. a.

- alle Unterlagen, mit deren Hilfe die Korrektheit der Daten, die Zulässigkeit ihrer Verarbeitung und die Beachtung der Rechte der Betroffenen beurteilt werden kann,

- alle Unterlagen über personelle, technische und organisatorische Vorkehrungen zur Verwirklichung des Datenschutzes,
- alle Verwaltungsvorschriften, Richtlinien, Dienstanweisungen, Verträge usw., die mit der Ausführung der Datenschutzvorschriften zu tun haben,
- alle Verarbeitungsprogramme sowie die Verfahrens-, Programm- und Systemdokumentationen.

38.3 Die Kontrollbefugnisse können sowohl vom TLfD persönlich als auch von seinen Mitarbeitern ausgeübt werden. Die Mitarbeiter müssen sich in üblicher Weise, etwa durch Vorlage des Dienstausweises, legitimieren. Bei den in § 13 Abs. 4 ThürDSG genannten Sicherheitsbehörden und Strafverfolgungsorganen müssen sie darüber hinaus einen schriftlichen, d. h. vom TLfD unterzeichneten Spezialauftrag vorlegen.

Zu § 39 ThürDSG

39.1 Der TLfD hat keine unmittelbaren Weisungsbefugnisse gegenüber den Stellen der öffentlichen Verwaltung. Nach § 39 Abs. 1 ThürDSG steht ihm vielmehr ein Beanstandungsrecht zu, wenn er Verletzungen von Vorschriften des ThürDSG, sonstiger Vorschriften des Datenschutzes oder sonstige Mängel bei der Verarbeitung und Nutzung personenbezogener Daten (z. B. Mängel in der Datensicherheit) feststellt. Die Behebung der Beanstandung bleibt dem Träger der beanstandeten Stelle überlassen. Die Form der Beanstandung richtet sich nach den gegebenen Umständen. Ersatzvornahme oder ähnliche Zwangsmittel sind dem TLfD verwehrt.

39.2 Verstreicht die zur Behebung der Beanstandung gesetzte Frist ohne Erfolg, dann wendet sich der TLfD an die für die Sicherstellung des Datenschutzes nach § 34 ThürDSG verantwortliche Stelle und die Aufsichtsbehörde und fordert Abhilfemaßnahmen (§ 34 Abs. 2 ThürDSG). Wird die Beanstandung auch dann nicht abgestellt, dann verständigt der TLfD den Landtag und die Landesregierung.

Zu § 40 ThürDSG

Neben seiner Kontrolltätigkeit und der Unterstützung Betroffener bei der Wahrnehmung ihres Rechts auf informationelle Selbstbestimmung berät der TLfD insbesondere den Landtag, die Landesregierung, aber auch alle öffentlichen Stellen zu Fragen bei der Durchsetzung des Datenschutzes. Diesem Ziel dient auch der von ihm alle zwei Jahre dem Landtag gegenüber zu erstattende Bericht über seine Tätigkeit.

Zu § 42 ThürDSG

Aufsichtsbehörde für die Datenverarbeitung im nicht öffentlichen Bereich nach § 38 Abs. 6 BDSG ist das Thüringer Landesverwaltungsamt (§ 6 der Zweiten Verordnung zur Bestimmung von Zuständigkeiten im Geschäftsbereich des Thüringer Innenministeriums, GVBl. 1992 S. 66). Die Kontrolle öffentlicher Stellen, die am Wettbewerb teilnehmen, obliegt dem TLfD (§ 37 ThürDSG).

Zu § 43 ThürDSG

Die nach bisher geltendem Recht vorliegende Beschränkung des Antragsrechts auf den Betroffenen, als dem in seinem Persönlichkeitsrecht Verletzten, hat in den Fällen Probleme aufgeworfen, in denen der Betroffene von der Verletzung seines Persönlichkeitsrechts keine Kenntnis hatte. Die Einführung des Antragsrechts für den TLfD korrespondiert mit der gleichlautenden Bestimmung im BDSG, wonach dem Bundesbeauftragten für den Datenschutz in Umsetzung des Artikels 28 Abs. 3, dritter Spiegelstrich der EG-Datenschutzrichtlinie eine Anzeigebefugnis zusteht.

Thüringer Innenministerium
Referat 20a
Erfurt, 07.02.2003
Az.: 20a.15-1082.32

Anlagen

Anlage 1: Formblatt Verfahrensverzeichnis

Anlage 1a: Erläuterungen zum Formblatt

Anlage 2: Einrichtungen und Organe der ehemaligen DDR

Anlage 3a: Muster Freigabevermerk innerhalb der Ministerien

Anlage 3b: Muster Freigabevermerk anderer Behörden

Anlage 3c: Muster Freigabeschreiben durch Ministerium

Anlage 1

Verfahrensverzeichnis nach § 10 Thüringer Datenschutzgesetz

1. Angaben zur Daten verarbeitenden Stelle

1.1 Name und Anschrift
1.2 Abteilung, Referat
1.3 Bei Auftragsdatenverarbeitung: Verarbeitende Stelle
1.4 Nähere Auskunft erteilt (Ansprechpartner):

2. Angaben zum automatisierten Verfahren

2.1 Bezeichnung des Verfahrens und Kurzbezeichnung
2.2 Örtlicher Geltungsbereich
2.3 Verfahren wird eingesetzt ab/seit:

2.4 Aufgabe, zu deren Erfüllung die Daten verarbeitet werden
2.5 Rechtsgrundlage der Verarbeitung
2.6 Kreis der Betroffenen
2.7 Regelfristen für die Löschung der Daten/Prüfung der Löschung

Datum:..... Unterschrift: .....

3. Art der gespeicherten Daten

Lfd. Nr.	Bezeichnung der Daten

Datum: ..... Unterschrift: .....

4. Regelmäßige Datenübermittlungen und automatisierte Abrufe

4.1 Empfänger (innerhalb, außerhalb, Drittländer)	
4.2 Rechtsgrundlage der Übermittlung	
4.3 Kreis der Betroffenen	
4.4 Art der übermittelten Daten	
Lfd. Nr.	Bezeichnung der Daten

Blatt __/__

Datum:..... Unterschrift: .....

5. Interne Angaben zum Verfahren

5.1 Verarbeitungsberechtigte Personen oder Personengruppen
5.2 Beschreibung der eingesetzten Hard- und Software (ggf. Querverweis zum Inventarverzeichnis)
5.3 Beschreibung der besonderen Maßnahmen nach § 9 Abs. 2 ThürDSG

Datum:..... Unterschrift: .....

Erläuterungen zum Formblatt „Verfahrensverzeichnis“

1. Allgemeine Bemerkungen

Nach § 10 Abs. 1 ThürDSG führen die Daten verarbeitenden Stellen ein Verzeichnis der automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden. § 10 Abs. 2 ThürDSG legt fest, welche Angaben mindestens über automatisierte Verfahren zu dokumentieren sind:

1. Name und Anschrift der Daten verarbeitenden Stelle,
2. die Bezeichnung des Verfahrens,
3. die Aufgabe, zu deren Erfüllung personenbezogene Daten verarbeitet werden und die Rechtsgrundlage der Verarbeitung,
4. die Art der gespeicherten Daten,
5. der Kreis der Betroffenen,
6. die Art der regelmäßig zu übermittelnden Daten und deren Empfänger sowie geplante Übermittlungen in Drittstaaten,
7. die Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung,
8. die verarbeitungsberechtigten Personen oder Personengruppen,
9. eine allgemeine Beschreibung des Datenverarbeitungssystems, die eine vorläufige Beurteilung der Angemessenheit der nach § 9 getroffenen Maßnahmen erlaubt.

Auf eine nachhaltige Dokumentation im Verfahrensverzeichnis kann für bestimmte automatisierte Verfahren verzichtet werden, wenn eine Freigabe nach

- § 34 Abs. 3 Satz 1 Nr. 3 ThürDSG
  „...deren einziger Zweck das Führen eines Registers ist, das auf Grund einer Rechtsvorschrift zur Information der Öffentlichkeit bestimmt ist,“

  oder
- § 34 Abs. 3 Satz 2 und 3 ThürDSG
  „[2]Einer Freigabe bedarf es ferner nicht, wenn das einzusetzende Verfahren unter Berücksichtigung der verarbeiteten oder genutzten Daten eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen nicht erwarten lässt. [3]Die Ministerien regeln jeweils für ihren Geschäftsbereich und für die unter ihrer Aufsicht stehenden juristischen Personen des öffentlichen Rechts durch Rechtsverordnung, bei welchen Verfahren und Stellen die Voraussetzungen nach Satz 2 erfüllt sind.“

gesetzlich nicht vorgeschrieben ist.

Das Verzeichnis kann mit Ausnahme der Angaben zu den Ziffern 8 und 9 von jedermann gebühren- und auslagenfrei eingesehen werden. Dies gilt nicht für Verfahrensverzeichnisse der Verfassungsschutzbehörden sowie bei Vorliegen von Versagungsgründen nach § 13 Abs. 5 ThürDSG.

2. Besonderheiten

Die Ausnahmen von der formellen Dokumentationspflicht sind in § 10 ThürDSG geregelt. Soweit eine Daten verarbeitende Stelle nach § 10a Abs. 1 ThürDSG einen Beauftragten für den Datenschutz bestellt hat, ist dieser nach § 10a Abs. 2 Satz 3 Nr. 2 ThürDSG für die Führung des Verfahrensverzeichnisses zuständig. Dazu gehört auch das Bereithalten für die Einsichtnahme nach § 10 Abs. 3 ThürDSG. Die gründliche Wahrnehmung der Pflichten eines Beauftragten für den Datenschutz nach § 10a Abs. 2 Satz 3 Nr. 3 ThürDSG setzt allerdings in der Praxis voraus, dass für das Überwachen der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden, eine ständige und aktuelle Übersicht aller eingesetzten Verfahren existiert. Am einfachsten ist es, wenn diese Informationen auf dem Computer des Beauftragten für den Datenschutz maschinell verwaltet werden. Dadurch ist sichergestellt, dass die Dokumentation aktuell bleibt. Neben dem Verfahrensverzeichnis kann es sich um folgende ergänzende Informationsbereiche handeln: Verzeichnis der Benutzerberechtigungen (User-Kataster), Softwareverzeichnis, Verzeichnis über die Fälle von Auftragsdatenverarbeitung (Service-Kataster), Nachweis der datenschutzrechtlichen Freigabe und die Dokumentation von wichtigen Datenschutz- und Datensicherheitsproblemen (Problemregister, Sicherheitskonzept, Risikoanalyse, Kontrollen des TLfD). Der Umfang der Aufgaben hängt von der konkreten Situation der Daten verarbeitenden Stelle ab und ist vom Beauftragten für den Datenschutz nach pflichtgemäßem Ermessen im Einvernehmen mit dem Behördenleiter festzulegen und wahrzunehmen.

3. Erläuterungen zu den Einzelangaben im Formblatt

3.1 Angaben zur Daten verarbeitenden Stelle

Ziffer 1.1:
Genauer Name und Anschrift der öffentlichen Stelle, für die die Daten verarbeitet werden (z. B. Gemeinde xy, Gemeinde xy der Verwaltungsgemeinschaft, Zweckverband z, Landesamt für ...), nicht Postfachadresse, nicht Computerstandort

Ziffer 1.2:
Bezeichnung der Organisationseinheit innerhalb der Stelle nach Ziffer 1.1

Ziffer 1.3:
Name und Anschrift des Auftragnehmers (z. B. Landesrechenzentrum, kommunales Gebietsrechenzentrum)

Ziffer 1.4:
Name und Funktion des Ansprechpartners, Tel.-Nr.

3.2 Angaben zum automatisierten Verfahren

Ziffer 2.1:
Allgemein verständliche Bezeichnung des Verfahrens (z. B. Wohngeldbewilligung, Automatisiertes Liegenschaftskataster, Personalinformationssystem, Schießleistungsnachweis)
Der datenschutzrechtliche Verfahrensbegriff ist an logischen Kriterien, wie Funktionalität, Zweckbindung, Verarbeitungslogik, Wirkung von Verknüpfungs- und Zugriffsregeln, orientiert. Die bloße Dokumentation der physische Datenorganisation (z. B. Datenbankstruktur oder Dateibeschreibung) leistet für das Herbeiführen datenschutzrechtlicher Transparenz keinen geeigneten Beitrag.
Die Kurzbezeichnung von max. 8 Stellen soll als Ordnungsmerkmal innerhalb des Verzeichnisses dienen. Die Bezeichnungssystematik wird von der Daten verarbeitenden Stelle nach den jeweiligen Erfordernissen, insbesondere unter Berücksichtigung der Anzahl von automatisierten Verfahren, selbst festgelegt.

Ziffer 2.2:
Angaben über den örtlichen Geltungsbereich des Verfahrens (z. B. Freistaat Thüringen, Gemeindeverwaltung x, Landkreis y, Landratsamt z, Zweckverbandsgebiet, Landesamt für...)

Ziffer 2.3:
Zeitpunkt der erstmaligen Nutzung des Verfahrens

Ziffer 2.4:
Kurze und aussagekräftige Erläuterung der Inhalte und Aufgaben, für die das Verfahren nach Ziffer 2.1 eingesetzt wird

Werden die Daten für verschiedene Verarbeitungszwecke verwendet, sind diese einzeln aufzuführen. Nicht ausreichend transparent sind Sammelbegriffe wie Personalmanagement, Gemeindeverwaltung, Integrationsverfahren, Vorgangsverwaltung, Recherchesystem oder Controlling.

Ziffer 2.5:
Nennung der Rechtsnorm, aus der sich die Zulässigkeit der Verarbeitung der personenbezogenen Daten unmittelbar ergibt

Hilfsweise können Zuständigkeitsregelungen in Verbindung mit den allgemeinen Zulässigkeitsvoraussetzungen nach § 20 ThürDSG oder Hinweise auf Einwilligung der Betroffenen nach § 4 Abs. 1 ThürDSG oder Vorliegen einer Dienstvereinbarung angegeben werden.

Ziffer 2.6:
Beschreibung des von der Verarbeitung betroffenen Personenkreises (z.B. Einwohner, Bedienstete, Antragsteller, Anschluss- und Benutzungspflichtige, Leistungsempfänger, Beschwerdeführer, Tatverdächtige, Lieferanten)

Ziffer 2.7:
Explizite Angabe der Regelfristen für die Löschung der Daten oder für die Prüfung der Löschung

Sind die Fristen nicht durch Rechtsvorschriften bestimmt, hat die Daten verarbeitende Stelle Fristen unter Beachtung von § 16 Abs. 1 ThürDSG nach den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit selbst festzulegen.

3.3 Angaben zur Art der gespeicherten Daten

Die Aufgabe besteht in der Beschreibung der logischen Datenelemente des automatisierten Verfahrens, unter Umständen bis zur Einzelangabe (Feldebene), soweit es zur Erfüllung des datenschutzrechtlichen Transparenzgebotes erforderlich ist. Auf die Dokumentation von DV-technischen Daten wie Satznummer, Satzlänge, Bitleisten, Indextabellen oder Adressverweisen und verfahrensbedingt redundanter Daten ist zu verzichten. Sammelbegriffe sind nur zulässig, soweit sie nicht zu Unklarheiten führen (zulässig ist z. B. „Anschrift“ statt „Postleitzahl, Ort, Straße und Hausnummer“). Die Datenelemente sind einer systematischen Gliederung folgend durchzunummerieren. Die Ordnungsnummern der Daten sollen auch beim Einfügen oder Löschen von Datenelementen möglichst beibehalten werden. Soweit häufiger Änderungsbedarf absehbar ist, kann eine Nummerierung auch in Fünfer- oder Zehnerschritten vorgenommen werden.
Die Bezeichnung der Datenelemente soll aus sich heraus verständlich sein, kein IT-Fachwissen und keine vertieften Verwaltungskenntnisse voraussetzen oder Fachabkürzungen enthalten, die nicht offenkundig sind. Dies gilt insbesondere für Verfahren, die den Vollzug von Verwaltungsakten unterstützen oder direkt elektronische Verwaltungsdienstleistungen (zukünftig im Sinne von „e-Government“) für die Bevölkerung erbringen und demzufolge erhöhte Publizität erwarten lassen.
Die Bezeichnung soll ggf. erkennen lassen, ob die Mehrfachspeicherung von Sachverhalten (zeitliche Verläufe) möglich ist oder ob nur jeweils der letzte, aktuelle Stand enthalten ist. Bei Bedarf kann der zulässige Wertbereich der Daten oder/und der Datentyp (alphabetisch, numerisch, logisch, Datum, Zeit) angefügt werden.

3.4 Angaben zu regelmäßigen Datenübermittlungen und automatisierten Abrufen

Als regelmäßige Datenübermittlung i. S. von § 34 Abs. 2 ThürDSG ist jede regelmäßige Weitergabe personenbezogener Daten von der Daten verarbeitenden Stelle (z. B. Gemeinde, Landratsamt, Landesbehörde) an Dritte (andere öffentliche Stelle oder Private) anzusehen. Regelmäßige Datenübermittlungen liegen vor, wenn bestimmte Daten bei Eintritt allgemein festgelegter Voraussetzungen übermittelt werden, ohne dass die Daten verarbeitende Stelle hierüber im konkreten Einzelfall entscheidet. Dies ist z. B. dann der Fall, wenn bei jeder Geburt, jedem Sterbefall, zu bestimmten Terminen oder bei jedem Zu- oder Wegzug Daten übermittelt werden. Die Übermittlung von personenbezogenen Daten durch ein automatisiertes Abrufverfahren nach § 7 ThürDSG erfüllt den gleichen Tatbestand und ist wie eine regelmäßige Datenübermittlung zu dokumentieren. Bei dieser Übermittlungsart entscheidet nicht die Daten verarbeitende Stelle, sondern die abrufende Stelle über die Zulässigkeit der einzelnen Übermittlung.

Ziffern 4.1 bis 4.3:
Die Erläuterungen zu den Ziffern 1.1, 2.5 und 2.6 gelten sinngemäß für die Dokumentation der regelmäßigen Datenübermittlungen und automatisierten Abrufe zu 4.1 bis 4.3. Soweit aus einem Verfahren heraus mehrere regelmäßige Datenübermittlungen an verschiedene Empfänger vorgenommen werden, sind diese einzeln (mehrere Blätter zu Ziffer 4) zu dokumentieren. Zu unterscheiden ist zwischen internen Empfängern i. S. von § 7 Abs. 6 ThürDSG, Empfängern außerhalb der Daten verarbeitenden Stelle und Empfängern in Drittstaaten i. S. von § 23 Abs. 1 Satz 2 ThürDSG.

Ziffer 4.4:
Laufende Nummer und Beschreibung der übermittelten Datenart sind der Liste der gespeicherten Datenarten nach Ziffer 3 unverändert zu entnehmen. Insbesondere bei der Übermittlung einer Teilmenge von Daten ist wegen des erforderlichen eindeutigen Bezugs zu den gespeicherten Daten eine neue Nummerierung zu unterlassen.

3.5 Interne Angaben zum Verfahren

Die nachfolgend aufgeführten Daten sind vom Einsichtsrecht nach § 10 Abs. 3 ThürDSG ausgenommen.

Ziffer 5.1:
Die verarbeitungsberechtigten Personen können direkt, aber auch indirekt durch genaue Funktionsbezeichnung (z. B. Referatsleiter Personalwesen, Sachbearbeiter für Kassenwesen, Zentralabteilungsleiter, Sachbearbeiter Stadtarchiv, Mitglied Gutachterausschuss, Polizeiführer vom Dienst) benannt werden. Der Personenkreis ist auf den unabdingbar erforderlichen Umfang zu beschränken. Eine namentliche Festlegung kann bei Daten der Schutzstufe 2 geboten sein.

Ziffer 5.2:
Je nach Komplexität und Anwendungsbreite des Verfahrens und der Sensibilität der verarbeiteten Daten sind Angaben zur Hardware einzutragen (z. B. Gattungsbezeichnung der Datenverarbeitungsanlage, Arbeitsplatz- / Server-Konfiguration, exklusiver Einzelrechner mit Inventarnummer, PC mit lokalem Datennetz oder mit öffentlichem Datennetzanschluss, mobiler Rechner). Die Eintragung der Inventarnummer kommt dann in Betracht, soweit der sichere Betrieb des Verfahrens eine besondere Installation der Datenverarbeitungsanlage voraussetzt oder das Verfahren an einen bestimmten Arbeitsplatz gebunden ist. Angaben zur Software bestehen aus der Bezeichnung des Betriebssystems und der Anwendungssoftware, wobei Standardsoftware für Büro- und Laborumgebungen und Individualsoftware für spezielle Verfahren unterscheidbar sein soll. Der Verantwortliche für die Gestaltung der Anwendungssoftware muss zumindest in allgemeiner Form erkennbar sein (z. B. namhaftes Softwareprodukt, Eigenprogrammierung, Auftragsprogrammierung durch Softwarehaus xy, Nachnutzung von Bund/Ländern/Kommunen oder „eingeführter“ Name des Verfahrens).

Ziffer 5.3:
Hier sind alle technischen und organisatorischen Maßnahmen nach § 9 ThürDSG aufzuführen, die zusätzlich (d. h. über den Stand der Technik des IT-Grundschutzes hinaus) für das dokumentierte Verfahren getroffen, installiert und/oder implementiert wurden, z. B. Benutzerberechtigung auf Anwendungsebene mit Codewort/Codekarte/Biometrie, Vier-Augen-Prinzip bei Administratorberechtigungen, hardware- oder softwaremäßige Verschlüsselung für Datenspeicherung und Datenübertragung, Verwendung von digitalen Signaturen, abstrahlsichere Hardware, räumliche Abschottung (besonderer Zutritts- und Einbruchschutz, Zugangskontrolle), besonderes Backup- und Recovery-Regime, unterbrechungsfreier Betrieb, Protokollierung auf Anwendungsebene, Datenausgabe im verdeckten Druck, automatisches Kuvertieren u. ä.
Die Angaben dienen der vorläufigen Beurteilung der Datensicherheit und gleichzeitig der Revisionsfähigkeit der getroffenen Maßnahmen.
Soweit vorhanden, sollte auf die durchgeführte Bedrohungs- /Risikoanalyse und das Sicherheitskonzept konkret Bezug genommen werden.

Anlage 2

Beispielhafte Aufzählung ehemaliger staatlicher oder wirtschaftsleitender Organe, Kombinate, Betriebe oder Einrichtungen sowie gesellschaftliche Organisationen der Deutschen Demokratischen Republik

Ehemalige staatliche oder wirtschaftsleitende Organe, Kombinate, Betriebe oder Einrichtungen sowie gesellschaftliche Organisationen der Deutschen Demokratischen Republik (DDR) waren insbesondere:

- die Volksvertretungen, die zentralen und örtlichen Staatsorgane sowie deren nachgeordnete Einrichtungen (einschl. der Gerichte, Strafvollzugs- und Polizeibehörden),

- die Parteien:
  Sozialistische Einheitspartei Deutschlands (SED),
  Christlich-Demokratische Union (CDU),
  Liberal-Demokratische Partei Deutschlands (LDPD),
  National-Demokratische Partei Deutschlands (NDPD),
  Demokratische Bauernpartei Deutschlands (DBD),

- die mandatstragenden gesellschaftlichen Organisationen in den Volksvertretungen:
  die Nationale Front der DDR (NF),
  Freier Deutscher Gewerkschaftsbund (FDGB),
  Freie Deutsche Jugend (FDJ)
  Demokratischer Frauenbund Deutschlands (DFD),
  Kulturbund der DDR (KB),
  Vereinigung der gegenseitigen Bauernhilfe (VdgB),
  Konsumgenossenschaft der DDR (KG),

- sonstige Organisationen und Verbände:
  Arbeiter- und Bauerninspektion (ABI) einschließlich der
  Volkskontrollausschüsse,
  Blinden und Sehschwachen Verband der DDR (BSV),
  Bund der Architekten (BdA),
  Deutscher Turn und Sportbund der DDR (DTSB),
  Deutsches Rotes Kreuz der DDR (DRK),
  Gehörlosen und Schwerhörigen Verband der DDR (GSV),
  Gesellschaft für Deutsch-Sowjetische Freundschaft (DSF),
  Jagdgesellschaften
  Kammer der Technik (KdT),
  Schriftstellerverband der DDR,
  Solidaritätskomitee der DDR,
  URANIA der DDR
  Verband bildender Künstler der DDR (VBK),
  Verband der Journalisten der DDR (VDJ),
  Verband der Kleingärtner, Siedler und Kleintierzüchter (VKSK),
  Verband der Theaterschaffenden der DDR (VT),
  Vereinigung der Juristen der DDR (VdJ),
  Volkssolidarität (VS),
  wissenschaftliche und andere Gesellschaften,

- die paramilitärischen Organisationen:
  Gesellschaft für Sport und Technik (GST),
  Kampfgruppen der Arbeiterklasse sowie

- die Kombinate, volkseigene Betriebe und Einrichtungen sowie Genossenschaften.

Anlage 3a

(Mustertext für die Freigabe von Verfahren, die innerhalb oberster Behörden eingesetzt werden)

Referat XX
Az.:

Erfurt, ‚Datum'
Hausruf:
SB:

Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten nach § 34 Abs. 2 ThürDSG

Anlage: - Formblätter zum Verfahrensverzeichnis nach § 10 ThürDSG
- ggf. weitere ergänzende Unterlagen

1.) Vermerk

Für das Verfahren

„ ... (*Verfahrensbezeichnung gem. Ziff. 2.1. des Formblatts zum Verfahrensverzeichnis*) ... "

wird nach § 34 Abs. 2 ThürDSG die Freigabe beantragt. Aus fachlicher und datenschutzrechlicher Sicht sind die vorgesehenen Datenspeicherungen und die vorgesehenen Datenübermittlungen zulässig.

Name und Unterschrift
(Referatsleiter XX)

2.) Beauftragter für den Datenschutz des Ministeriums m.d.B. um Mitzeichnung

3.) Abteilungsleiter „X" m.d.B. um Freigabe

4.) Beauftragter für den Datenschutz des Ministeriums z.w.V.
(Aufnahme der Formblätter in das Verfahrensverzeichnis des Ministeriums)

5.) Referat XX z.d.A.

Anlage 3b

(Mustertext für die Freigabe von Verfahren, die in den Ministerien nachgeordneten Behörden eingesetzt werden)

Referat XX
Az.:

Erfurt, ‚Datum'
Hausruf:
SB:

Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten nach § 34 Abs. 2 ThürDSG

Anlage:
- Schreiben ‚der nachgeordneten Behörde (Behördenleiter)' vom ..., Az.: ....
- Formblätter zum Verfahrensverzeichnis nach § 10 ThürDSG
- Freigabeschreiben an ‚die nachgeordnete Behörde'

1.) Vermerk

Mit Schreiben vom ... hat ... (*Bezeichnung der nachgeordneten Behörde*) für das Verfahren

„ ... (*Verfahrensbezeichnung gem. Ziff. 2.1. des Formblatts zum Verfahrensverzeichnis*) ... "

die Freigabe nach § 34 Abs. 2 ThürDSG beantragt. Aus fachlicher und datenschutzrechlicher Sicht sind die vorgesehenen Datenspeicherung und die vorgesehenen Datenübermittlungen zulässig.

Name und Unterschrift
(Leiter des Fachaufsichtsreferats XX)

2.) Beauftragter für den Datenschutz des Ministeriums m.d.B. um Kenntnisnahme

3.) Abteilungsleiter „X" m.d.B. um Freigabe und Zeichnung des Freigabeschreibens

5.) Referat XX z.w.V.
(*Freigabeschreiben mit Anlagen an nachgeordnete Behörde*)

Anlage 3c

(Muster des Freigabeschreibens an die nachgeordnete Behörde)

(Adressat)

Thüringer Ministerium ...., Postfach ....., ... Erfurt

Freigabe automatisierter Verfahren zur Verarbeitung personenbezogener Daten nach § 34 Abs. 2 ThürDSG
hier: *(Verfahrensbezeichnung)*

Ihr Schreiben vom ..., Az.: ...

Anlagen: Formblätter zum Verfahrensverzeichnis nach § 10 ThürDSG

Freigabe

Dem mit Schreiben vom ... gestellten Antrag auf Freigabe des automatisierten Verfahrens

(Verfahrensbezeichnung)

wird gemäß § 34 Abs. 2 Thüringer Datenschutzgesetz zugestimmt. Aus fachlicher und datenschutzrechtlicher Sicht sind die vorgesehenen Datenspeicherungen und die vorgesehenen Datenübermittlungen zulässig.

Im Auftrag

Abteilungsleiter