Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

Handreichung zur Datenschutz-Folgenabschätzung (DS-FA) für den öffentlichen Bereich

Stand: Januar 2021

Inhalt

1. Einleitung

Mit der Datenschutz-Folgenabschätzung (DS-FA) verpflichtet die Datenschutz-Grundverordnung (DS-GVO) in Art. 35 Abs. 1 DS-GVO den Verantwortlichen vor einer Verarbeitung von personenbezogenen Daten, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen.

Eine DS-FA ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Durch den technikneutralen Ansatz des sachlichen Anwendungsbereiches der DS-GVO ist es ohne Belang, ob es sich um ein automatisiertes Verfahren oder um eine nichtautomatisierte Verarbeitung, z. B. in Papierakten handelt.

Dabei ist zu beachten, dass die DS-FA kein einmaliger Vorgang ist. Wenn Risiken (neu) hinzutreten oder sich Verarbeitungsvorgänge grundlegend ändern, muss erneut eine DS-FA durchgeführt werden. Somit wiederholt sich der Prozess der Datenschutz-Folgenabschätzung zyklisch und ermöglicht somit eine kontinuierliche Überprüfung und ggf. Anpassung der Verarbeitung personenbezogener Daten.

Die formellen Anforderungen an eine DS-FA sind in Art. 35 der DS-GVO geregelt. Weiterhin finden sich Hinweise auch in den Erwägungsgründen 84, 90, 91, 92 und 93 der DS-GVO. Die Methodik der Durchführung einer DS-FA wird in der DS-GVO nicht festgelegt. Hier besteht ein gewisser Spielraum für die Verantwortlichen. Es ist jedoch ratsam, bestehende Methoden oder Standards zu verwenden, zum Beispiel das Standard-Datenschutzmodell.

Gemäß § 13 Abs. 1 ThürDSG ist zu beachten, dass unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen immer ein Datenschutzbeauftragter für die öffentliche Stelle zu benennen ist. Bei der Erstellung einer Datenschutz-

Folgenabschätzung ist nach Art. 35 Abs. 2 DS-GVO i. V. m. § 15 Abs. 2 Satz 3 ThürDSG der Rat des Datenschutzbeauftragten einzuholen.
Neben der DS-GVO sieht die JI-Richtlinie, die im Thüringer Datenschutzgesetz (ThürDSG) im dritten Abschnitt (§§ 31 – 53 ThürDSG) umgesetzt wurde, eine Datenschutz-Folgenabschätzung im § 52 ThürDSG vor.

Die JI-Richtlinie bzw. das ThürDSG kommt immer dann zum Tragen, wenn die öffentlichen Stellen, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten zuständig sind, personenbezogene Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche. Die Verhütung von Straftaten im Sinne des § 31 Satzes 1 ThürDSG umfasst den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit. Die Sätze 1 und 2 des § 31 ThürDSG finden zudem Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 Strafgesetzbuch (StGB), von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder von Geldbußen zuständig sind. Soweit dieser Abschnitt Bestimmungen für Auftragsverarbeiter enthält, gilt er auch für diese (§ 31 ThürDSG).

Ebenso wie bei der DS-FA nach der DS-GVO ist auch der Datenschutzbeauftragte bei einer DS-FA nach § 52 ThürDSG zu beteiligen (§ 52 Abs. 3 i. V. m. § 15 Abs. 2 Satz 3 ThürDSG).

Es empfiehlt sich daher, im Vorfeld zu prüfen, ob die DS-FA auf Grundlage der DS-GVO (z. B. Eingliederungshilfe für seelisch behinderte Kinder) oder nach dem ThürDSG (z. B. Verarbeitung personenbezogener Daten im Rahmen der Aufdeckung von Straftaten) durchzuführen ist. Zur Orientierung kann die nachfolgende Tabelle dienen:

Abgrenzung	DS-FA nach DS-GVO	DS-FA nach ThürDSG
Anwendungsbereich	Art. 2 und 3 DS-GVO	§ 31 ThürDSG
formelle Anforderung	Art. 35 DS-GVO	§ 52 ThürDSG
Hinweise zur Durchführung	Erwägungsgründe 84, 90, 91, 92 und 93 der DS-GVO	Erwägungsgründe 53 und 58 der JI-Richtlinie sowie die Begründung zu § 52 ThürDSG
Miteinbeziehung Datenschutzbeauftragter	Art. 35 Abs. 2 DS-GVO i. V. m. § 15 Abs. 2 Satz 3 ThürDSG	§ 52 Abs. 3 ThürDSG i. V. m. § 15 Abs. 2 Satz 3 ThürDSG

2. Prüfungsschema

Die Durchführung einer Datenschutz-Folgenabschätzung erfolgt im Wesentlichen in zwei Schritten; Erstens: einer Vorprüfung, die auch Schwellwertanalyse genannt wird, und Zweitens: bei identifizierter Notwendigkeit, die eigentliche Durchführung der DS-FA.

Schritt 1 – Vorprüfung, ist eine Datenschutz-Folgenabschätzung notwendig?

Die Schwellwertanalyse immer vor der Einführung eines neuen bzw. bei einer wesentlichen Änderung eines bestehenden Verarbeitungsvorgangs durchzuführen.

Wer führt die Vorprüfung zur Datenschutz-Folgenabschätzung durch?
Da eine DS-FA ein umfassender Prozess ist, ist es notwendig, beim Verantwortlichen ein interdisziplinär besetztes Prüfteam zusammenzustellen. Die Teammitglieder sollten über Kenntnisse zum Datenschutz, zur Risikoermittlung und über die Fachprozesse verfügen.

Der Verantwortliche gemäß Art. 4 Nr. 7 DS-GVO bzw. § 32 Nr. 7 ThürDSG, vertreten durch das Prüfteam, führt die Vorprüfung durch; der Datenschutzbeauftragte berät ihn dabei, Art. 35 Abs. 2 DS-GVO i. V. m. § 15 Abs. 2 Satz 3 ThürDSG bzw. § 52 Abs. 3 i. V. m. § 15 Abs. 2 Satz 3 ThürDSG. Relevante Interessengruppen, zum Beispiel der Personalrat, sind einzubeziehen.

Wann ist eine Datenschutz-Folgenabschätzung durchzuführen?
Gemäß Art. 35 Abs. 1 DS-GVO bzw. § 52 Abs. 1 ThürDSG ist eine DS-FA immer dann durchzuführen, wenn die Form der Verarbeitung, insbesondere bei

- Verwendung **neuer Technologien**,
- aufgrund der **Art**, des **Umfangs**,
- der **Umstände** und der **Zwecke** der Verarbeitung

voraussichtlich ein **hohes Risiko** für die **Rechte und Freiheiten natürlicher Personen** zur Folge hat.

Die DS-GVO nennt jedoch selbst keine Verfahren, die als neue Technologien anzusehen sind. Sie verweist vielmehr in Art. 35 Abs. 4 DS-GVO auf die zu erstellende Liste der Aufsichtsbehörden, für welche Fälle eine DS-FA verpflichtend durchzuführen ist, die sogenannte Black-List (vgl. Seite 10) Für den JI-Bereich sieht das ThürDSG eine solche Liste nicht vor, daher ist immer eine DS-FA durchzuführen, wenn die Voraussetzungen des § 52 Abs. 1 ThürDSG erfüllt sind.

Weiterhin ist gemäß Art. 35 Abs. 3 DS-GVO eine DS-FA insbesondere in folgenden Fällen erforderlich:

a) **systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen**, die sich auf automatische Verarbeitung, einschließlich **Profiling** gründet und die **ihrerseits als Grundlage für Entscheidungen dient**, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen (z. B. Profiling, Scoring, automatisierte Einzelentscheidungen).
b) **Umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten** gemäß **Art. 9 Abs. 1 DS-GVO** (dazu zählen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung) oder gemäß **Art. 10 DS-GVO** von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.
c) Systematische umfangreiche **Überwachung öffentlich zugänglicher Bereiche** (z. B.: umfangreiche Videoüberwachung in Einkaufszentren oder Schwimmbädern).

Die frühere europäische Artikel-29-Datenschutzgruppe hat zudem in ihren Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine

Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (Workingpaper 248)[1], **9 Kriterien** benannt, die bei der Bewertung zu berücksichtigen sind:

1. Bewertung und Einstufung,
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung,
3. Systematische Überwachung,
4. Vertrauliche Daten oder höchst persönliche Daten,
5. Datenverarbeitung in großem Umfang,
6. Abgleichen oder Zusammenführen von Datensätzen,
7. Daten zu schutzbedürftigen Betroffenen (ErwGr. 75 DS-GVO bzw. Erwägungsgrund 51 JI-Richtlinie),
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen,
9. Fälle, in denen die Verarbeitung an sich „die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert“ (Art. 22 und ErwGr. 91 DS-GVO).

Treffen mindestens zwei der genannten Kriterien auf einen Verarbeitungsvorgang zu, muss der Verantwortliche in den meisten Fällen zu dem Ergebnis kommen, dass eine DS-FA notwendig ist. Je mehr Kriterien ein Verarbeitungsvorgang erfüllt, umso höher ist die Wahrscheinlichkeit, dass ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht.
Es kann aber auch Fälle geben, in denen der Verantwortliche bei Erfüllung nur eines Kriteriums von der Notwendigkeit einer DS-FA ausgehen muss.

Andererseits kann es auch vorkommen, dass ein Verantwortlicher einen Verarbeitungsvorgang, der den vorgenannten Kriterien entspricht, nicht als Vorgang bewertet,

[1] Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, Stand 04.10.2017, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Publikationen/DokumenteArt29Gruppe_EDSA/Guidelines/WP248_LeitlinienZurDatenschutzFolgenabschaetzung.pdf?__blob=publicationFile&v=2

der „wahrscheinlich ein hohes Risiko mit sich bringt“. In einem solchen Fall muss der Verantwortliche begründen und dokumentieren, warum er keine DS-FA durchführt, und den Standpunkt des Datenschutzbeauftragten mit einbeziehen bzw. festhalten.

Zur Bewertung des Umfangs von Verarbeitungsvorgängen, empfiehlt die Artikel-29-Datenschutzgruppe folgende Faktoren zu berücksichtigen:

a. Zahl der Betroffenen (konkrete Anzahl oder als Anteil an einer Gruppe),
b. verarbeitete Datenmenge bzw. Menge der verschiedenartigen Datenelemente,
c. Dauer oder Dauerhaftigkeit der Datenverarbeitung,
d. geografisches Ausmaß der Datenverarbeitung.

Weiterhin ist eine DS-FA zwingend in den Fällen durchzuführen, die in der **Liste der Verarbeitungstätigkeiten, für die eine DS-FA durchzuführen ist,** welche von den Aufsichtsbehörden veröffentlicht wurde (Art. 35 Abs. 4 DS-GVO), aufgeführt sind. Diese „**Black-List“** finden Sie für Thüringen unter: https://www.tlfdi.de/mam/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf.

Vorprüfung der DS-FA nach der DS-GVO:

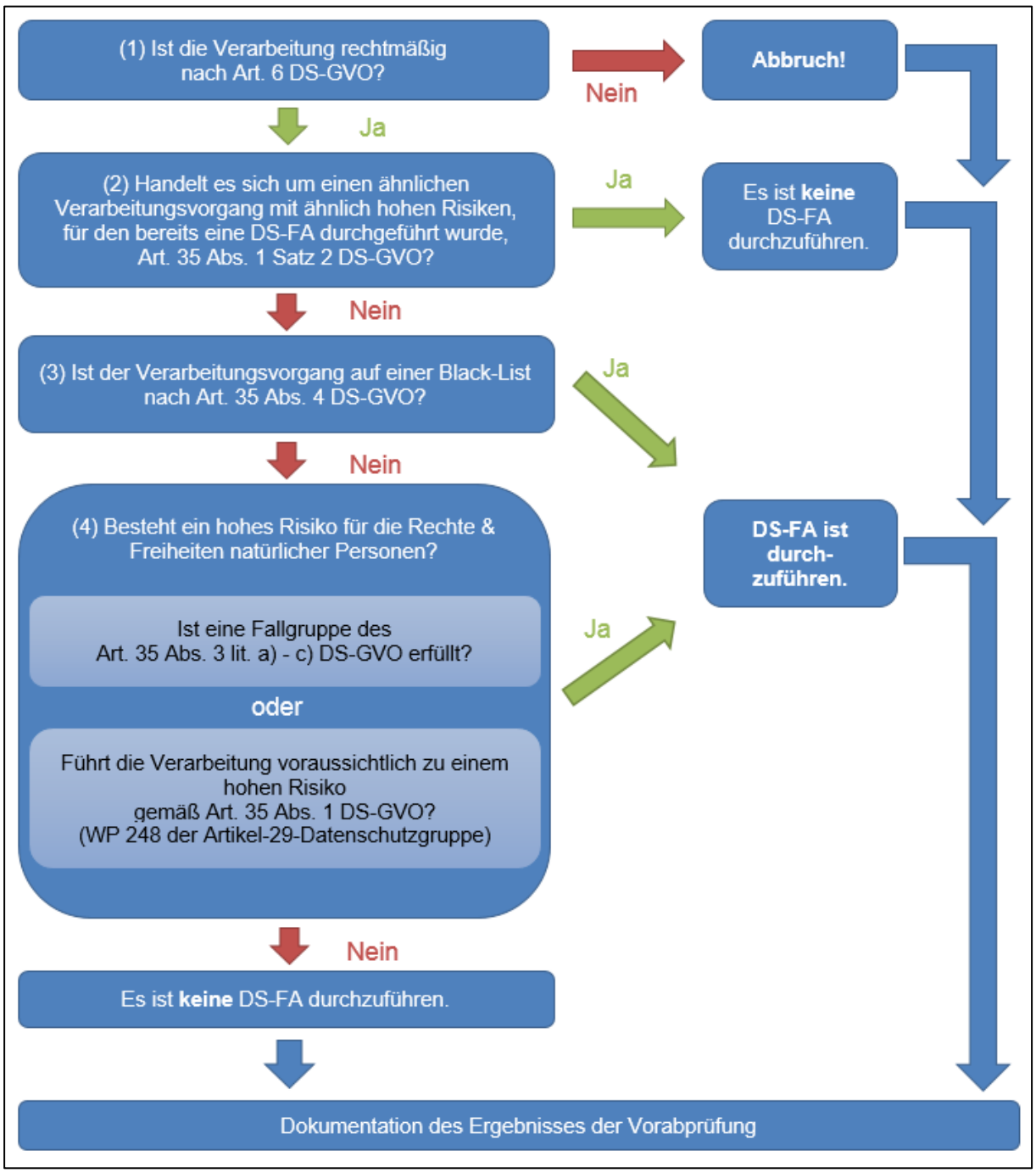

Abbildung 1 - Übersicht der Vorprüfung zur Notwendigkeit einer DS-FA für den öffentlichen Bereich, Stand September 2020

Vorprüfung der DS-FA nach dem ThürDSG:

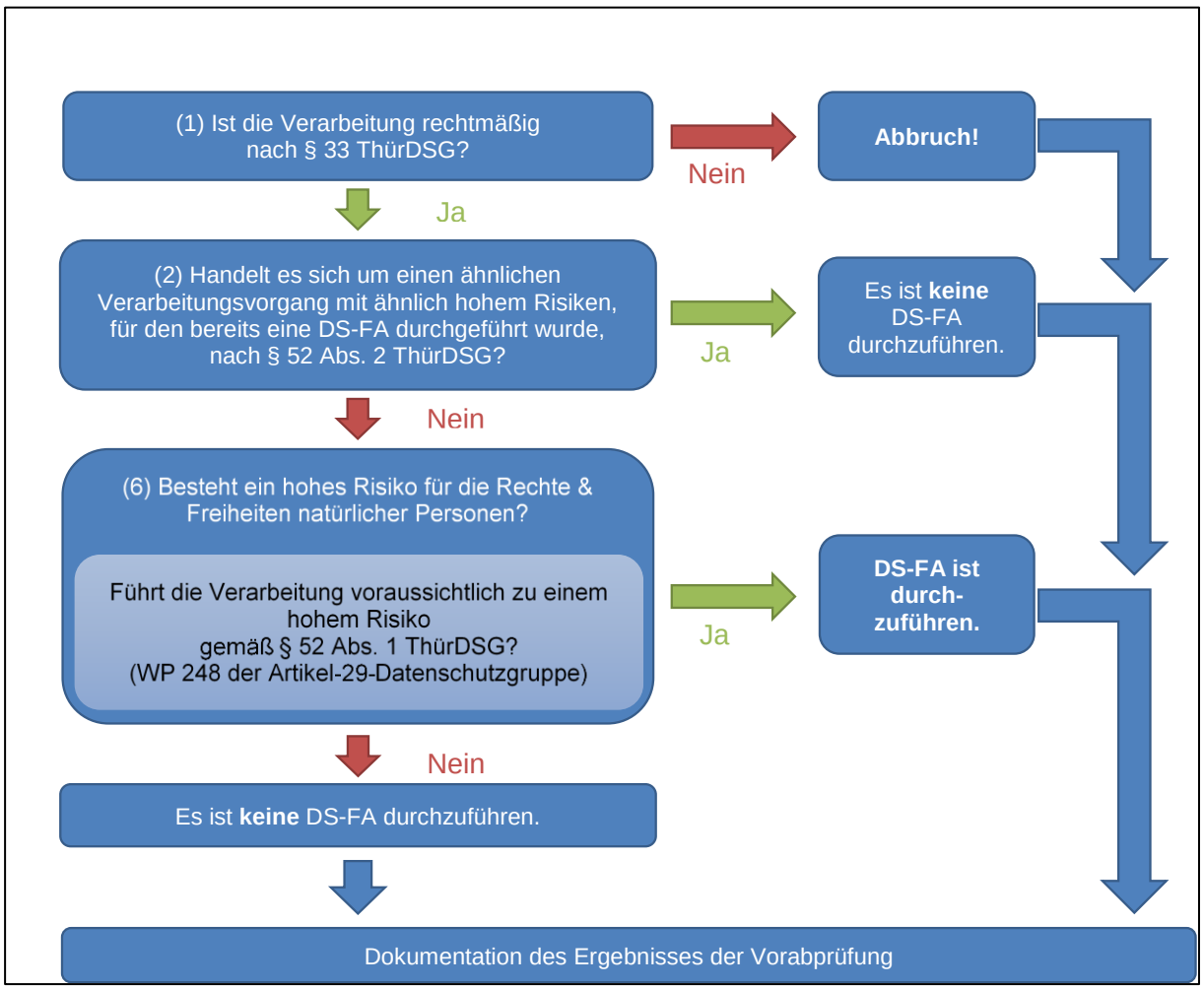

Abbildung 2 - Übersicht der Vorprüfung zur Notwendigkeit einer DS-FA nach ThürDSG für den öffentlichen Bereich, Stand September 2020

Schritt 2 – Durchführung der DS-FA nach Art. 35 DS-GVO bzw. § 52 ThürDSG

Wer führt die Datenschutz-Folgenabschätzung durch?

Für die Datenschutz-Folgenabschätzung ist, wie für die Vorprüfung, ein interdisziplinär besetztes Team um den Verantwortlichen im Sinne Art. 4 Nr. 7 DS-GVO bzw. § 32 Nr. 7 ThürDSG zuständig. Der Datenschutzbeauftragte hat eine beratende Funktion inne (Art. 35 Abs. 2 DS-GVO i. V. § 15 Abs. 2 Satz 3 ThürDSG bzw. § 52 Abs. 3 i. V. m. § 15 Abs. 2 Satz 3 ThürDSG).

Ferner sind wiederum die Interessensgruppen zu beteiligen und ggf. der Standpunkt der betroffenen Personen oder ihrer Vertreter einzuholen, wenn die DS-FA auf der Grundlage der DS-GVO erfolgt (Art. 35 Abs. 9 DS-GVO). Dies kann zum Beispiel der Personalrat sein. Eine Beteiligung von Interessensgruppen sieht die DS-FA nach § 52 ThürDSG nicht vor.

Was gehört in eine Datenschutz-Folgenabschätzung?

Der Mindestumfang einer Datenschutz-Folgenabschätzung auf Grundlage der DS-GVO ist in Art. 35 Abs. 7 DS-GVO geregelt und umfasst:

- eine **systematische Beschreibung** der
  - geplanten **Verarbeitungsvorgänge** und
  - **Zwecke** der Verarbeitung,
  - ggf. die vom Verantwortlichen verfolgten **berechtigten Interessen**,
- eine **Bewertung** der **Notwendigkeit** und **Verhältnismäßigkeit** der Verarbeitungsvorgänge in **Bezug auf den Zweck**,
- **Bewertung** der **Risiken** für die Rechte und Freiheiten der **betroffenen Personen[2],**
- die zur Bewältigung der Risiken **geplanten Abhilfemaßnahmen**, einschließlich **Garantien**, **Sicherheitsvorkehrungen** und **Verfahren**, durch die der Schutz personenbezogener Daten sichergestellt und der **Nachweis** dafür erbracht wird, dass die DS-GVO eingehalten wird, wobei den Rechten und **be-**

[2] Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 26.04.2018, abrufbar unter https://www.tlfdi.de/mam/tlfdi/datenschutz/dsk_kpnr_18_risiko.pdf

rechtigten Interessen der **betroffenen Person** und **sonstiger Betroffener** Rechnung getragen wird.

Zudem geben die Erwägungsgrunde 84, 89 bis 93 der DS-GVO wichtige Hinweise zur Umsetzung. Das Ergebnis der Datenschutz-Folgenabschätzung, einschließlich der getroffenen technischen und organisatorischen Maßnahmen, ist revisionssicher zu dokumentieren. Für die Beschreibung der Verarbeitungsvorgänge empfiehlt es sich bspw. auch Grafiken und Ablaufpläne, wie z. B. Datenflussdiagramme, einzusetzen.

Der Mindestumfang einer Datenschutz-Folgenabschätzung auf Grundlage des ThürDSG ist in § 52 Abs. 4 ThürDSG geregelt und umfasst:

- eine **systematische Beschreibung** der
  - geplanten **Verarbeitungsvorgänge** und
  - **Zwecke** der Verarbeitung,
  - ggf. die vom Verantwortlichen verfolgten **berechtigten Interessen,**
- eine **Bewertung** der **Notwendigkeit** und **Verhältnismäßigkeit** der Verarbeitungsvorgänge in **Bezug auf den Zweck,**
- **Bewertung** der **Gefahren** für die Rechtsgüter der **betroffenen Personen**[3]**,**
- die **Maßnahmen**, mit denen bestehenden Gefahren abgeholfen werden soll, einschließlich der **Garantien**, der **Sicherheitsvorkehrungen** und der **Verfahren**, durch die der **Schutz personenbezogener Daten sichergestellt** und die **Einhaltung** der gesetzlichen Vorgaben **nachgewiese**n werden soll.

Zudem geben die Erwägungsgrunde 53 und 58 der JI-Richtlinie wichtige Hinweise zur Umsetzung. Das Ergebnis der Datenschutz-Folgenabschätzung, einschließlich der getroffenen technischen und organisatorischen Maßnahmen, ist revisionssicher zu dokumentieren. Für die Beschreibung der Verarbeitungsvorgänge empfiehlt es

[3] Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 26.04.2018, abrufbar unter https://www.tlfdi.de/mam/tlfdi/datenschutz/dsk_kpnr_18_risiko.pdf

sich bspw. auch Grafiken und Ablaufpläne, wie z. B. Datenflussdiagramme, einzusetzen.

Wie wird eine DS-FA durchgeführt?

Um eine DS-FA durchzuführen, kann der Verantwortliche auf verschiedene Methoden (Standard-Datenschutzmodell[4] (SDM), ISO/IEC 29134 und weitere) zurückgreifen. Entscheidend ist, dass die gewählte Methode die in der DS-GVO sowie im ThürDSG aufgeführten Mindestanforderungen an eine Datenschutz-Folgenabschätzung erfüllt. Der TLfDI empfiehlt die Anwendung der Methodik des Standard-Datenschutzmodells. Dieses überführt die Grundsätze für die Verarbeitung personenbezogener Daten im Sinne des Art. 5 Abs. 1 DS-GVO:

- Transparenz,
- Zweckbindung,
- Datenminimierung,
- Richtigkeit,
- Speicherbegrenzung,
- Integrität und Vertraulichkeit

sowie weitere Anforderungen der DS-GVO in die sieben Gewährleistungsziele des SDM:

- Datenminimierung,
- Verfügbarkeit,
- Integrität,
- Vertraulichkeit,
- Nichtverkettung,
- Transparenz,
- Intervenierbarkeit

und weist mit der enthaltenen Risikoanalyse die Erfüllung der Gewährleistungsziele und damit nach, ob ein Verarbeitungsvorgang den Anforderungen der DS-GVO ge-

[4] Das Standard Datenschutzmodell - Eine Methode zur Datenschutzberatung und –prüfung auf der Basis einheitlicher Gewährleistungsziele, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 17.04.2020, abrufbar unter https://tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/sdm-methode_v20b.pdf

nügt. Der Ablauf einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO sowie nach § 52 ThürDSG gliedert sich wiederum in verschiede Phasen:

Phase 1 – Vorbereitung

In der Vorbereitungsphase erfolgt die systematische Beschreibung der Verarbeitungstätigkeiten, diese sollte umfassen:

- eine Beschreibung unter Angabe der evtl. auch eingesetzten Techniken, Art, Umfang und Umstände der Verarbeitung (siehe auch Art. 30 DS-GVO bzw. § 50 ThürDSG, Verzeichnis der Verarbeitungstätigkeiten),
- eine Beschreibung des Umfangs, der Anzahl und Häufigkeit des Datenabrufs sowie Bestimmung der Umstände des Datenabrufs,
- Beschreibung der Verarbeitungsvorgänge in Hinblick auf den Zweck, sofern möglich sollte beschrieben werden, was die Verarbeitungstätigkeit nicht leisten soll (Zweckabgrenzung),
- Angabe der am Verarbeitungsvorgang Beteiligten (z. B. Mitarbeiter, IT-Nutzer, Administratoren, Auftragsverarbeiter),
- bei IT-Systemen auch die Beschreibung der Systemgrenzen und Schnittstellen.

Phase 2 – normative Bewertung und Risikobewertung

In dieser Phase erfolgt zunächst eine:

(a) **normative Bewertung** der Verarbeitungsvorgänge gemäß Art. 35 Abs. 7 Buchst. b) DS-GVO bzw. § 52 Abs. 4 Nr. 2 ThürDSG: Dazu stellt man die Notwendigkeit der Verarbeitung dar und prüft, ob die Verhältnismäßigkeit zwischen Zweck und Verarbeitungsvorgängen gewahrt bleibt. Hierzu sollte man sich z. B. die Frage stellen, ob es zum Erreichen des Zwecks nicht Verarbeitungsvorgänge gibt, die mit weniger personenbezogenen Daten auskommen (Schutzziel: Datenminimierung). Anschließend erfolgt die Risikobewertung.

(b) **Risikobewertung**[5] gemäß Art. 35 Abs. 1 DS-GVO bzw. § 52 Abs. 1 ThürDSG: Hierbei erfolgt eine detaillierte Risikobewertung in Bezug auf die zu erwartende Beeinträchtigung für die Rechte und Freiheiten natürlicher Personen.

Die DS-GVO selbst definiert den Begriff des Risikos nicht. Im Kurzpapier Nr. 18 der DSK wird der Begriff wie folgt definiert: „Ein Risiko im Sinne der DS-GVO ist das Bestehen der Möglichkeit des Einritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann."
Zur Art des Schadens führt Erwägungsgrund 75 DS-GVO bzw. Erwägungsgrund 51 JI-Richtlinie aus, dass dieser sowohl physischer, materieller oder immaterieller Art sein kann. Als mögliche Schäden werden aufgeführt:

- Diskriminierung,
- Identitätsdiebstahl oder -betrug,
- finanzieller Verlust,
- Rufschädigung,
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten,
- unbefugte Aufhebung der Pseudonymisierung,
- erhebliche wirtschaftliche und gesellschaftliche Nachteile.

Die Risikobewertung selbst ist in folgenden Schritten durchzuführen:

- Risikoidentifikation (Ereignis, Risikoquelle, Schaden),
- Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden für die Rechte und Freiheiten betroffener Personen (Anhand objektiver Kriterien),
- Zuordnung zu Risikoabstufungen.

[5] Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 26.04.2018, abrufbar unter https://www.tlfdi.de/mam/tlfdi/datenschutz/dsk_kpnr_18_risiko.pdf

Im Rahmen der Risikoidentifikation ist zu klären, welche Schäden für die betroffenen natürlichen Personen auf Grundlage der verarbeiteten Daten bewirkt werden, wodurch (Ereignis) kann es zum Schaden kommen und durch welche Handlungen und Umstände (Risikoquelle) kann es zum Eintritt der Ereignisse kommen. Es sind also die Schäden, Ereignisse und Risikoquellen zu identifizieren und zu beschreiben. Als Kurzformel hilft „X löst Y aus und führt zu Z“.
Im nächsten Schritt erfolgt die Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden.

Die DS-GVO und das ThürDSG verlangen, dass Risiken anhand objektiver Kriterien zu beurteilen sind (ErwGr. 76 DS-GVO bzw. Begründung zu 52 ThürDSG). Hierfür bietet es sich an, die Schwere möglicher Schäden und die Eintrittswahrscheinlichkeiten in Stufen einzuordnen (geringfügig, überschaubar, substanziell, groß). Weiterhin muss der Verantwortliche objektive Kriterien festlegen, auf deren Basis die Einordung in die Stufen erfolgt. Die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten betroffener Personen sollte in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden. Die im Folgenden aufgeführte Einstufung ist als Beispiel anzusehen und so nicht als Grundlage für die Risikobetrachtung in einer DS-FA heranzuziehen.

Für die Eintrittswahrscheinlichkeit könnte die Einstufung beispielsweise wie folgt aussehen:

Eintrittswahrscheinlichkeit	Vergangenheit	Zukunft
geringfügig	durchschnittlich einmal 10 Jahren	erwartet alle 10 Jahre
überschaubar	durchschnittlich einmal in 5 Jahre	erwartet alle 5 Jahre
substanziell	durchschnittlich einmal im Jahr	erwartet jährlich
groß	durchschnittlich einmal im Monat	erwartet monatlich

Nachdem die Einstufungen für die Eintrittswahrscheinlichkeit festgelegt wurden, sind nun die Kriterien für die Einstufungen der Schadenshöhe zu definieren. DSK Kurzpapier Nr. 18[6] führt Beispiele möglicher Schäden auf, welche für die Klassifikation herangezogen werden können.

[6] Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 26.04.2018, abrufbar unter https://www.tlfdi.de/mam/tlfdi/datenschutz/dsk_kpnr_18_risiko.pdf

Ein unvollständiges Beispiel wäre:

Schwere des potentielle. Schadens	Diskriminierung	Identitätsdiebstahl o. -betrug	finanzieller Verlust	Rufschädigung	wirtschaftliche od. gesellschaftliche Nachteile	Gefahr für Leib- und Leben	(weitere Schäden)
geringfügig			ein Monatsgehalt		keine bis geringe Nachteile	keine bis geringe gesundheitliche Beeinträchtigungen	
Überschaubar			mehrere Monatsgehälter		spürbare Auswirkungen für den Betroffenen die zu kleinen Nachteilen führen	körperliche Verletzungen / zeitweilige Gesundheitliche Beeinträchtigungen	
substanziell	in Teilbereichen, z.B. Arbeitsplatz		ein Jahresgehalt	In Teilbereichen, z.B. Arbeitsplatz	Auswirkungen haben Nachteile für den Betroffenen in Alltag	dauerhafte gesundheitliche Beeinträchtigungen / Schwere körperliche Verletzung	
Groß	im gesamten Lebensumfeld	Identitätsdiebstahl	Verlust aller Vermögenswerte	im gesamten Lebensumfeld	Auswirkungen haben große Nachteile für den Betroffenen und sein persönliches Umfeld	Lebensgefahr	

Nachdem nun die identifizierten Risiken hinsichtlich Schwere des Schadens und Eintrittswahrscheinlichkeit klassifiziert wurden, erfolgt die Zuordnung zu den Risikostufen.

Dazu kann folgende Risikomatrix verwendet werden:

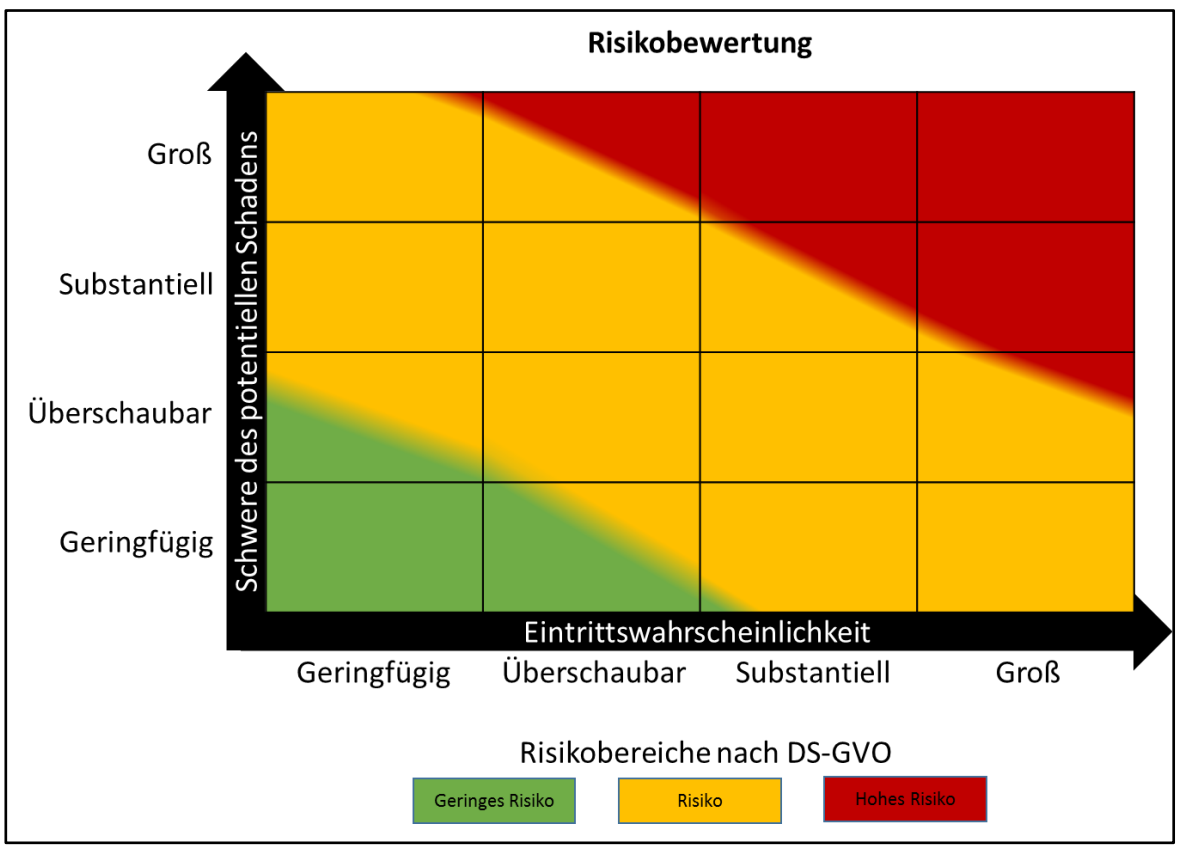

Abbildung 3 – Risikomatrix für die Abschätzung des Risikos in Anlehnung an Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 26.04.2018

Es empfiehlt sich, die Risikobewertung in Tabellen zu dokumentieren. Im Ergebnis hat man für jeden Verarbeitungsvorgang die Risikobewertung durchgeführt.

Beschreibung des Vorfalls		**Beschreibung des Schadens**	**Schwere des pot. Schadens**	**Eintrittswahrscheinlichkeit**	**Risikoeinstufung**
Risikoquelle	Ereignis				
der Mitarbeiter gibt eine falsche Anschrift im System ein		Wahlunterlagen können nicht zugestellt werden, weshalb der Betroffene sein Wahlrecht nicht ausüben kann	substantiell	groß	hohes Risiko

Phase 3 – Maßnahmen

In der Maßnahmenphase wird festgelegt, mit welchen Maßnahmen man den identifizierten Risiken entgegenwirken will. Dabei kann mit Hilfe der Maßnahmen die Eintrittswahrscheinlichkeit und / oder die Auswirkungen reduziert werden. Hilfestellung bieten hier die generischen Maßnahmen des Standard-Datenschutzmodells sowie der Referenzmaßnahmenkatalog[7] zum Standard Datenschutzmodell (SDM).

Beispiele für technische und organisatorische Maßnahmen:

- Zutrittskontrollsysteme,
- Türsicherung,
- Kennwortverfahren,
- Automatische Benutzersperren,
- Zwei-Faktor-Authentifizierung,
- Verschlüsselung von Daten und Datenträgern,

[7] Abrufbar unter https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/

- Pseudonymisierung von Daten,
- Differenziertes Berechtigungskonzept,
- Elektronische Signaturen,
- Back-Up-Verfahren,
- Festlegung von Verhaltensregeln,
- Regelmäßige Schulungen und Fortbildungen.

Mögliche weitere technischen und organisatorischen Maßnahmen (TOMs) finden Sie z. B. in ausführlicher Form im „IT-Grundschutz-Kompendium“[8] des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Auch wenn diese nur auf den IT-Grundschutz der IT-Sicherheit abzielen, so sind die Informationen dennoch hilfreich.

Phase 4 – Bericht

In der Berichtsphase werden die Ergebnisse der Phase 3 und 4 zusammengetragen und in einem Bericht zusammengefasst. Im Ergebnis ist zu bewerten, ob trotz aller getroffenen Maßnahmen weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Dieses Ergebnis ist im Bericht zu dokumentieren. Die Praxis hat gezeigt, dass Aufgrund der notwendigen Überarbeitungen und Wiederholungen von Datenschutz-Folgenabschätzungen es empfehlenswert ist, den Bericht in Tabellenform zu erstellen.

[8] IT-Grundschutz-Kompendium abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.pdf;jsessionid=60C886B9E61D665CEEDB611997CE8B3C.2_cid369?__blob=publicationFile&v=5

Die Fortsetzung des obigen Beispiels könnte wie folgt aussehen:

Beschreibung des Vorfalls		**Beschreibung des Schadens**	**Schwere des pot. Schadens**	**Eintrittswahrscheinlichkeit**	**Risikoeinstufung**	**Maßnahme**	**Schwere des pot. Schadens**	**Eintrittswahrscheinlichkeit mit Maßnahme**	**Risikoeinstufung**
Risikoquelle	Ereignis								
der Mitarbeiter gibt eine falsche Anschrift ein		Wahlunterlagen können nicht zugestellt werden, weshalb der Betroffene sein Wahlrecht nicht ausüben kann	substantiell	groß	hohes Risiko	Sichtprüfung der Eingegebenen Daten durch den Betroffenen	substantiell	geringfügig	geringes Risiko

Nach dem Standard-Datenschutzmodell folgt aus der initialen Risikoeinstufung der Schutzbedarf. Hier im Beispiel würde aus dem hohen Risiko in der ersten Risikobewertung ein hoher Schutzbedarf folgen. Dieser bleibt gem. Standard-Datenschutzmodell auch immer gleich. Für das Beispiel aus obiger Tabelle bedeutet dies, dass durch die Umsetzung der geplanten Maßnahme ein geringes Restrisiko verbleibt, das erreichte Schutzniveau ist demzufolge angemessen.

Führen die Verarbeitungsvorgänge trotz aller getroffenen Maßnahmen **weiterhin zu einem hohen Risiko** für die Rechte und Freiheiten der betroffenen natürlichen Personen, so ist **vor der Verarbeitung die Aufsichtsbehörde zu konsultieren** (Art. 36 Abs. 3 DS-GVO bzw. § 53 Abs. 1 ThürDSG). Auch dies ist zu dokumentieren.

Der Bericht über die durchgeführte Datenschutz-Folgenabschätzung ist vom Verantwortlichen aufzubewahren.

Phase 5 – Umsetzung der Maßnahmen und Prüfung der Wirksamkeit

Nach der Durchführung der Datenschutz-Folgenabschätzung folgt die Umsetzung der geplanten Maßnahmen, mit der Prüfung, ob die Maßnahmen auch die angenommene Wirkung entfalten. Hierzu sind vom Verantwortlichen entsprechende Tests durchzuführen sowie die Umsetzung und die Testergebnisse zu dokumentieren. Führen die geplanten Maßnahmen nicht zum gewünschten Ergebnis oder zeigen sich in den Test neue Risiken, ist die DS-FA erneut mit weiteren technischen und organisatorischen Maßnahmen durchzuführen.

Liegt die vollständige Dokumentation mit dem DS-FA-Bericht und der Bestätigung der Wirksamkeit der Maßnahmen vor, entscheidet der Verantwortliche gemäß Art. 4 Nr. 7 DS-GVO bzw. § 32 Nr. 7 ThürDSG über den Einsatz des Verfahrens.

Die Datenschutz-Folgenabschätzung ist ein kontinuierlicher Prozess, der während der gesamten Dauer der Verarbeitungsvorgänge stattfindet. So muss entweder anlassbezogen, z. B. vor Einführung eines neuen Verarbeitungsprozesses (Art. 35

Abs. 1 DS-GVO bzw. § 52 Abs. 1 ThürDSG) oder bei Änderung in den Verarbeitungsvorgängen oder bei den Risiken (Art. 35 Abs. 11 DS-GVO) sofort wieder in das o. g. Prüfungsschema zu Punkt 2 gegangen werden. Auch nach einer Beschwerde, kann eine erneute Risikoanalyse zur Notwendigkeit einer DS-FA führen. In jedem Fall sollte regelmäßig geprüft werden, ob die Annahmen bzgl. der Risiken noch gültig sind und ob die getroffenen Maßnahmen noch ihre Wirksamkeit entfalten.

3. Konsultation der Aufsichtsbehörde nach Art. 36 DS-GVO bzw. § 53 ThürDSG

Kommt der Verantwortliche bei der Gesamtbewertung der DS-FA zu dem Ergebnis, dass trotz aller getroffenen Maßnahmen weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht, hat der Verantwortliche die zuständige Aufsichtsbehörde zu konsultieren (Art. 36 DS-GVO bzw. § 53 ThürDSG).

Folgende Informationen sind gemäß Art. 36 Abs. 3 DS-GVO bzw. § 53 Abs. 2 ThürDSG bei der Konsultation beizulegen:

a) gegebenenfalls **Angaben** zu den jeweiligen **Zuständigkeiten** des **Verantwortlichen**, der **gemeinsam Verantwortlichen** und der an der Verarbeitung beteiligten **Auftragsverarbeiter**,
b) die **Zwecke** und die **Mittel** der beabsichtigten **Verarbeitung**,
c) die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß der DS-GVO bzw. des ThürDSG vorgesehenen **Maßnahmen** und **Garantien**,
d) gegebenenfalls die **Kontaktdaten** des **Datenschutzbeauftragten** bzw. bei der DS-FA nach § 52 ThürDSG muss die Angabe erfolgen,
e) die **Datenschutz-Folgenabschätzung** gemäß Artikel 35 DS-GVO bzw. § 52 ThürDSG und
f) alle **sonstigen** von der Aufsichtsbehörde **angeforderten Informationen**.

Die Aufsichtsbehörde muss im Falle einer DS-FA nach Art. 35 DS-GVO und kann im Falle einer DS-FA nach § 52 ThürDSG innerhalb der gesetzlichen Frist dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter eine schriftliche Empfehlung unterbreiten. Wichtig ist, darauf zu achten, ob es sich um eine DS-FA nach Art. 35 DS-GVO oder um eine DS-FA nach § 52 ThürDSG handelt, da sich die Fristberechnungen unterscheiden ebenso wie die rechtliche Verpflichtung.

Für die DS-FA nach Art. 35 DS-GVO gilt für die Fristberechnung der Art. 36 Abs. 2 DS-GVO. Die Aufsichtsbehörde muss nach Eingang des Ersuchens innerhalb von acht Wochen mit einer schriftlichen Empfehlung reagieren. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um bis zu sechs Wo-

chen verlängert werden, dazu muss der Verantwortliche innerhalb des ersten Monats unter Angabe der Gründe von der Aufsichtsbehörde informiert werden. Die Frist kann ausgesetzt werden, wenn zur Bewertung benötigte Informationen nachgefordert werden müssen.

Hingegen gilt für die DS-FA nach § 52 ThürDSG bei der Fristberechnung der § 53 Abs. 3 ThürDSG. Die Aufsichtsbehörde kann nach Eingang des Ersuchens innerhalb von sechs Wochen mit einer schriftlichen Empfehlung reagieren. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um einen Monat verlängert werden, dazu muss der Verantwortliche innerhalb des ersten Monats unter Angabe der Gründe von der Aufsichtsbehörde informiert werden.
Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung vor Eingang der schriftlichen Empfehlungen des Landesbeauftragten für den Datenschutz beginnen. In diesem Fall sind die Empfehlungen des Landesbeauftragten für den Datenschutz im Nachhinein zu berücksichtigen und die Art und Weise der Verarbeitung gegebenenfalls anzupassen (§ 53 Abs. 4 ThürDSG).

Am Ende der Konsultation kann die Aufsichtsbehörde:

a) Vorschläge zur Risikoeindämmung unterbreiten (Art. 36 Abs. 2 DS-DVO bzw. § 53 Abs. 3 ThürDSG),
b) anweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen (Art. 58 Abs. 2 Buchst. d) DS-GVO),
c) eine vorrübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, verhängen (Art. 58 Abs. 2 Buchst. f) DS-GVO),
d) eine Beanstandung erlassen, wenn gegen die Vorschriften des Datenschutzes bei einer DS-FA nach § 52 ThürDSG verstoßen wird (§ 7 Abs. 6 ThürDSG).

4. Komprimierte grafische Übersicht des Gesamtprozesses der DS-FA

Ablauf der DS-FA nach der DS-GVO:

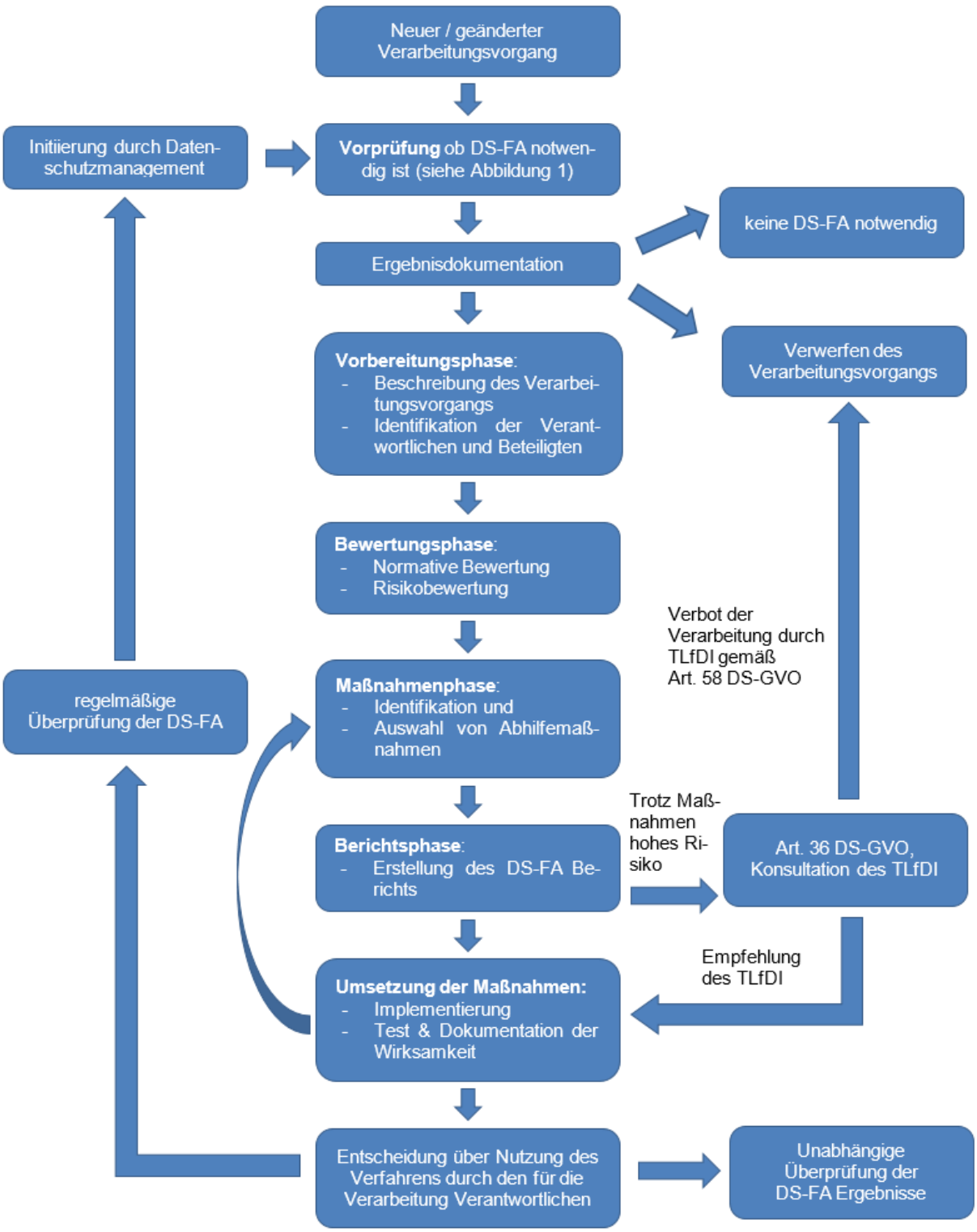

Abbildung 4 - grafische Übersicht DS-FA Prozess nach DS-GVO

Ablauf der DS-FA nach dem ThürDSG:

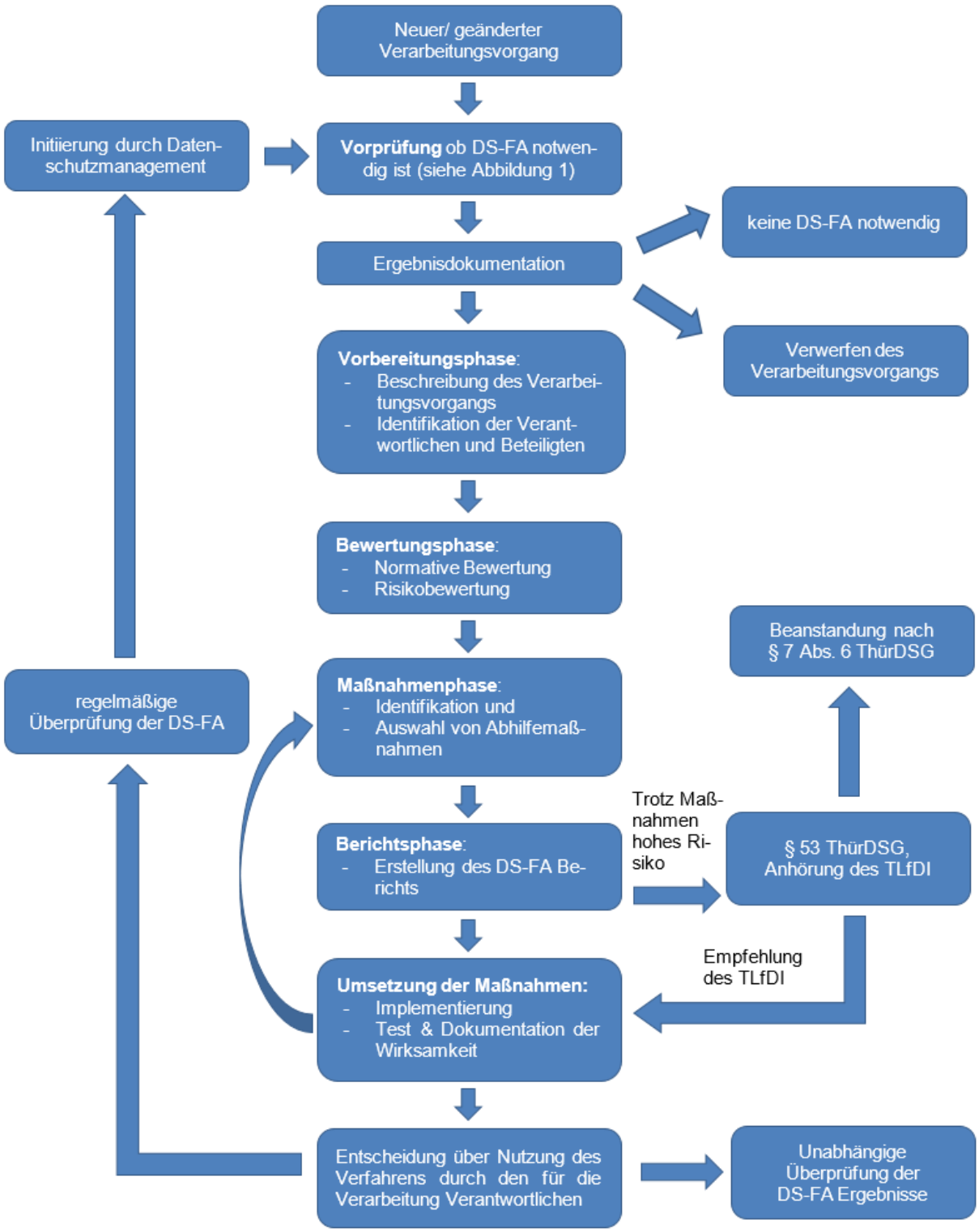

Abbildung 5 - grafische Übersicht DS-FA Prozess nach ThürDSG

5. Weiterführende Informationen und Quellen

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DS-GVO), abrufbar unter:
http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE

Bundesdatenschutzgesetz (BDSG) vom 30.06.2017, abrufbar unter:
https://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf

Thüringer Datenschutzgesetz vom 06.06.2018, abrufbar unter:
https://www.thueringen.de/mam/th3/tim/datenschutz/gesetz-und-verordnungsblatt-nr-06-2018.pdf

Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI Richtlinie), abrufbar unter:
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0680&from=EN

Kurzpapier Nr. 5: Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 24.07.2017, abrufbar unter:
https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_5_datenschutz-folgenabschatzung.pdf

Kurzpapier Nr. 8: Maßnahmenplan DS-GVO für Unternehmen, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 26.07.2017, abrufbar unter:
https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_8_massnahmenplan.pdf

Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 26.04.2018, abrufbar unter:
https://www.tlfdi.de/mam/tlfdi/datenschutz/dsk_kpnr_18_risiko.pdf

Das Standard-Datenschutzmodell, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Version 2.0b Stand April 2020 , abrufbar unter:

https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/sdm-methode_v20b.pdf

Vorläufige Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DS-GVO, Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit, Stand 04.07.2018, abrufbar unter:
https://www.tlfdi.de/mam/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf

Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Artikel 30 Abs. 1 DSGVO, Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit, Stand 2018, abrufbar unter:
https://www.tlfdi.de/mam/tlfdi/themen/muster_verarbeitungsverzeichnis_verantwortlicher.pdf

Hinweise zum Verzeichnis von Verarbeitungstätigkeiten, Art. 30 DS-GVO, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand Februar 2018, abrufbar unter:
https://www.tlfdi.de/mam/tlfdi/themen/hinweise_zum_verzeichnis_von_verarbeitungstatigkeiten.pdf

Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, Artikel-29-Datenschutzgruppe, Stand 04.10.2017, abrufbar unter:
https://www.datenschutzkonferenz-online.de/media/wp/20171004_wp248_rev01.pdf

IT-Grundschutz-Kompendium Zweite Edition Februar 2020, Bundesamt für Sicherheit in der Informationstechnik, Stand Februar 2020, abrufbar unter:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html