Thüringer Landesbeauftragter
für den Datenschutz und die Informationsfreiheit

Handreichung zur Datenschutz-Folgenabschätzung (DS-FA) nicht-öffentlicher Bereich

-

Art. 35 DS-GVO

Stand: September 2019

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 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 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 § 38 Abs. 1 BDSG ist zu beachten, dass unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen immer ein Datenschutzbeauftragter zu benennen ist, wenn ein Verantwortlicher Verarbeitungen vornimmt, die einer DS-FA nach Art. 35 DS-GVO unterliegen.

2. Prüfungsschema

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

Schritt 1 – Vorprüfung, ist eine DS-FA notwendig?

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, vertreten durch das Prüfteam, führt die Vorprüfung durch, der Datenschutzbeauftragte berät ihn dabei, Art. 35 Abs. 2 DS-GVO und relevante Interessengruppen (Stakeholder) sind einzubeziehen.

Wann ist eine Vorprüfung durchzuführen?
Gemäß Art. 35 Abs. 1 DS-GVO 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. Dabei nennt die DS-GVO 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.

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 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] 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

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 (Erwägungsgrund 75 DS-GVO)
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 Erwägungsgrund 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, 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.

Art. 35 Abs. 5 DS-GVO erlaubt den jeweiligen Aufsichtsbehörden eine Liste der Arten von Verarbeitungsvorgängen, zu veröffentlichen, für die keine DS-FA notwendig ist. Diese **„White-List“** ist zum aktuellen Stand nicht vorhanden. Offen bleibt auch die Frage, ob bzw. wann es eine deutsche White-List geben wird.

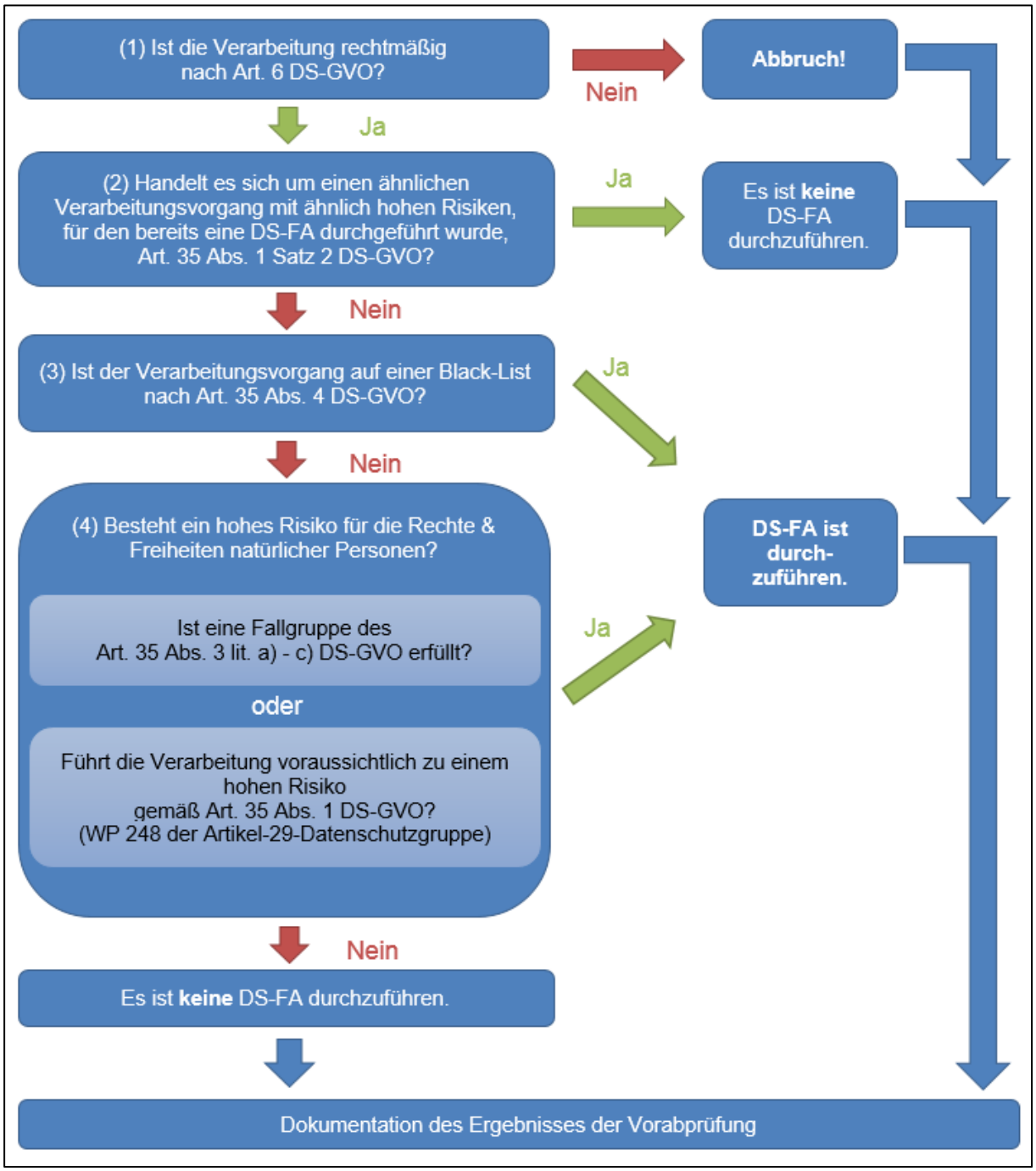

Abbildung 1 - Übersicht der Vorprüfung zur Notwendigkeit einer DS-FA für den nicht-öffentlichen Bereich, Stand Juni 2019

Schritt 2 – Durchführung der DS-FA nach Art. 35 DS-GVO

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 zuständig. Der Datenschutzbeauftragte hat eine beratende Funktion inne (Art. 35 Abs. 2 DS-GVO). Ferner sind wiederum die Stakeholder zu beteiligen und ggf. der Standpunkt der betroffenen Personen oder ihrer Vertreter einzuholen (Art. 35 Abs. 9 DS-GVO). Dies kann zum Beispiel der Betriebsrat sein.

Was gehört in eine Datenschutz-Folgenabschätzung?

Der Mindestumfang einer Datenschutz-Folgenabschätzung 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 **berechtigten Interessen** der **betroffenen Person** und **sonstiger Betroffener** Rechnung getragen wird.

[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

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.

Wie wird eine DS-FA durchgeführt?

Um eine DS-FA durchzuführen, stehen verschiedene Methoden (Standard-Datenschutzmodell (SDM), ISO/IEC 29134 und weitere) zur Verfügung. Neben den Grundsätzen für die Verarbeitung personenbezogener Daten gemäß Art. 5 Abs. 1 DS-GVO:

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

empfiehlt der TLfDI die Methodik des Standard-Datenschutzmodells einzusetzen. Der Ablauf einer Datenschutz-Folgenabschätzung 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, 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
- 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 lit. b) DS-GVO: 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**[3] gemäß Art. 35 Abs. 1 DS-GVO: 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 aus, dass dieser sowohl physischer, materieller oder immaterieller Art sein kann. Als mögliche Schäden werden aufgeführt:

- Diskriminierung,
- Identitätsdiebstahl oder -betrug,

[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

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

Nach Erwägungsgrund 76 DS-GVO sollte das Risiko anhand einer objektiven Bewertung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.
Dabei sind erstens die Schwere des Schadens in Bezug auf die Schutzziele (siehe SDM) und zweitens die Wahrscheinlichkeit, dass das Ereignis und Folgeschäden eintreten ins Verhältnis zu setzen. Dazu sind folgende Schritte durchzuführen:

1. **Risikoidentifikation**
2. **Abschätzung** von **Eintrittswahrscheinlichkeit** und **Schwere** möglicher Schäden
3. **Zuordnung** zu Risikoabstufungen

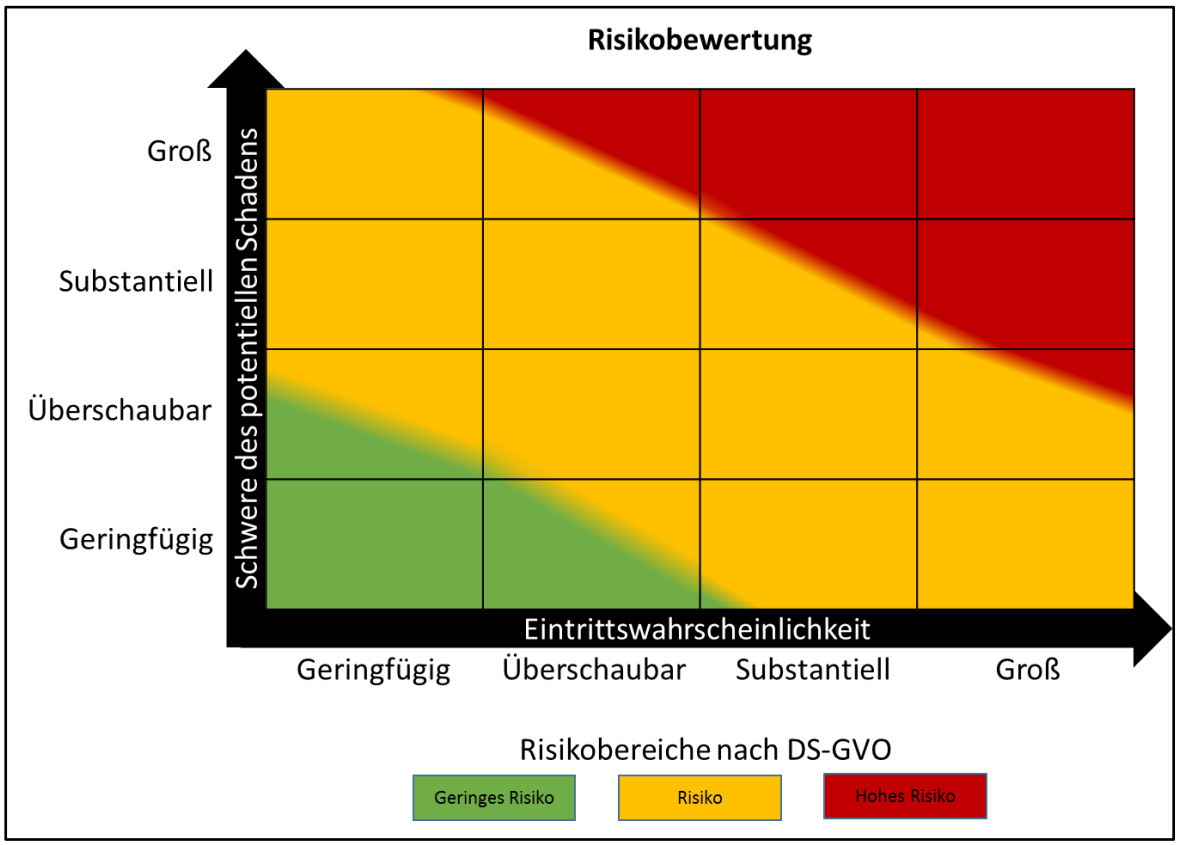

Abbildung 2 – Risikomatrix für die Abschätzung des Risikos in Anlehnung an Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen, Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK), Stand 26.04.2018

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 bietet hier der Maßnahmenkatalog[4] zum Standard Datenschutzmodell (SDM). Werden besonderer Kategorien personenbezogener Daten verarbeitet, nennt § 22 Abs. 2 Bundesdatenschutzgesetz (BDSG) mögliche Maßnahmen.

Beispiele für technische und organisatorische Maßnahmen:

- Zutrittskontrollsysteme
- Türsicherung

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

- Kennwortverfahren
- Automatische Benutzersperren
- Zwei-Faktor-Authentifizierung
- Verschlüsselung von Daten und Datenträgern
- 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. im „Routenplaner: Cyber-Sicherheit für Handwerksbetriebe“[5] sowie in ausführlicher Form im „IT-Grundschutz-Kompendium“[6] 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.

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). Auch dies ist zu dokumentieren.

---

[5] ROUTENPLANER: Cyber-Sicherheit für Handwerksbetriebe., Kompetenzzentrum Digitales Handwerk Zentralverband des Deutschen Handwerks (ZDH), Stand März 2019, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/ACS/routenplaner_print.html?nn=10027584

[6] 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

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 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) 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

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).

Folgende Informationen sind gemäß Art. 36 Abs. 3 DS-GVO bei der Konsultation beizulegen:

a) gegebenenfalls **Angaben** zu den jeweiligen **Zuständigkeiten** des **Verantwortlichen**, der **gemeinsam Verantwortlichen** und der an der Verarbeitung beteiligten **Auftragsverarbeiter**, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen,
b) die **Zwecke** und die **Mittel** der beabsichtigten **Verarbeitung**,
c) die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen **Maßnahmen** und **Garantien**,
d) gegebenenfalls die **Kontaktdaten** des **Datenschutzbeauftragten**,
e) die **Datenschutz-Folgenabschätzung** gemäß Artikel 35 und
f) alle **sonstigen** von der Aufsichtsbehörde **angeforderten Informationen**.

Nach Eingang des Ersuchens muss die Aufsichtsbehörde innerhalb von 8 Wochen mit einer schriftlichen Empfehlung reagieren (Art. 36 Abs. 2 DS-GVO). Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung um bis zu 6 Wochen verlängert werden, dazu muss der Verantwortliche innerhalb des ersten Monats unter Angabe der Gründe von der Aufsichtsbehörde informiert werden (Art. 36 Abs. 2 DS-GVO). Die Frist kann ausgesetzt werden, wenn zur Bewertung benötigte Informationen nachgefordert werden müssen.

Am Ende der Konsultation kann die Aufsichtsbehörde:

a) Vorschläge zur Risikoeindämmung unterbreiten (Art. 36 Abs. 2 DS-DVO),
b) anweisen Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen (Art. 58 Abs.2 lit. d) DS-GVO),
c) eine vorrübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, verhängen (Art. 58 Abs. 2 lit. f) DS-GVO).

4. Komprimierte grafische Übersicht des Gesamtprozesses der DS-FA

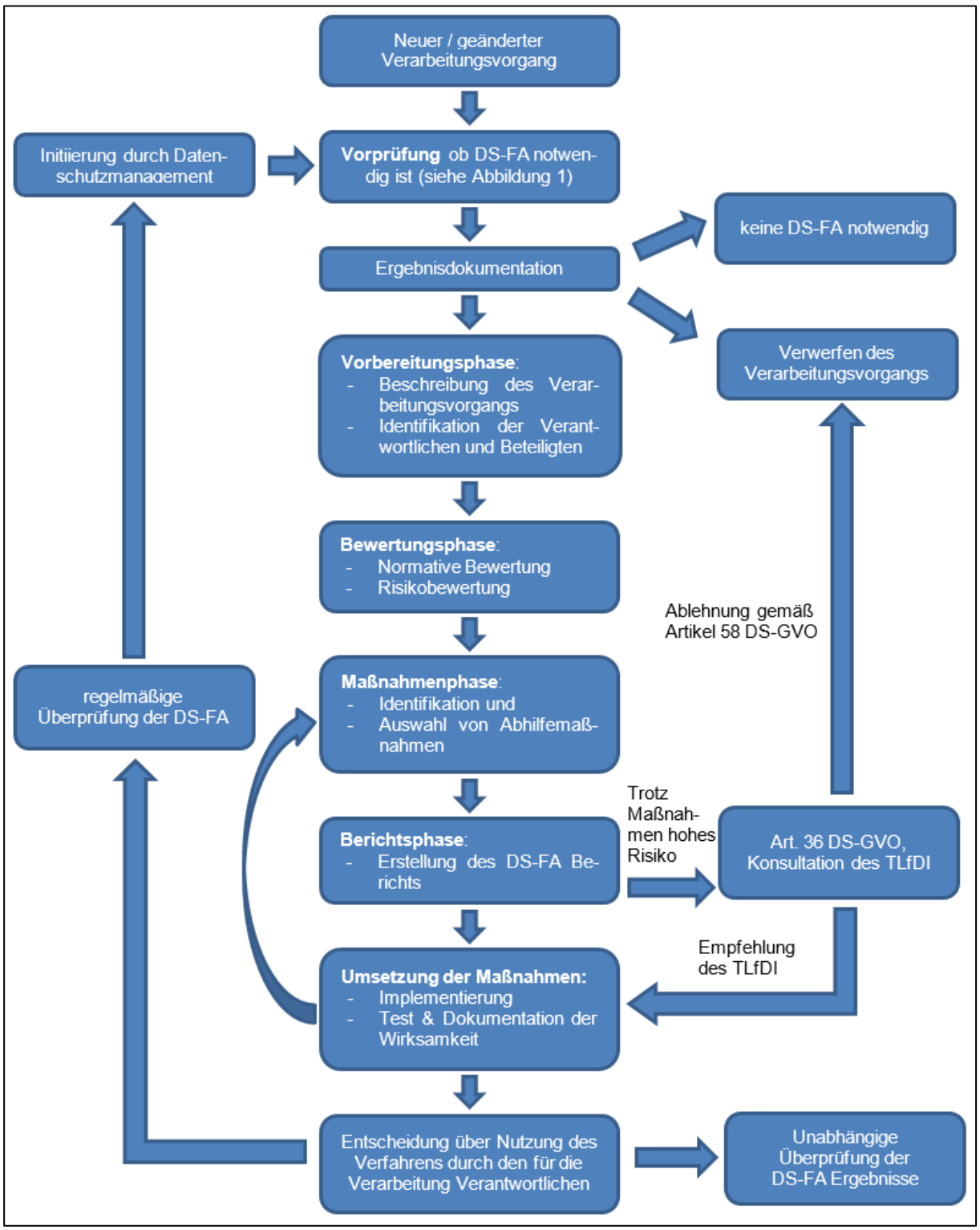

Abbildung 3 - grafische Übersicht DS-FA Prozess

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.tlfdi.de/mam/tlfdi/datenschutz/bdsg_neu.pdf

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

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), Stand 25/26.04.2018, abrufbar unter:
https://www.tlfdi.de/mam/tlfdi/gesetze/orientierungshilfen/sdm_v-1-1_broschure.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

ROUTENPLANER: Cyber-Sicherheit für Handwerksbetriebe., Kompetenzzentrum Digitales Handwerk Zentralverband des Deutschen Handwerks (ZDH), Stand März 2019, abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/ACS/routenplaner_print.html?nn=10027584

IT-Grundschutz-Kompendium Zweite Edition Februar 2019, Bundesamt für Sicherheit in der Informationstechnik, Stand Februar 2019, 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