Konferenz der unabhängigen

Datenschutzaufsichtsbehörden des Bundes und der Länder

Standardisierter Prüfprozess zu datenschutzrechtlichen Anforderungen bei EfA-Onlinediensten nach Onlinezugangsgesetz (OZG)

Stand:
Dezember 2025

Inhalt

1 Abkürzungsverzeichnis

1.1 Allgemein

Abs.	Absatz
Art.	Artikel
bzw.	beziehungsweise
d. h.	das heißt
DIN SPEC 66336	Qualitätsanforderungen für Onlineservices und -portale der öffentlichen Verwaltung (Servicestandard)
DSFA	Datenschutzfolgen-Abschätzung
DSK	Datenschutzkonferenz
f. / ff.	folgend
lit.	littera / Buchstabe
i. S. d.	im Sinne der/des
Nr.	Nummer
S.	Seite
s.o.	siehe oben
SDM	Standard-Datenschutz-Modell
SPS	Standardprozessschritt
TOMs	technische und organisatorische Maßnahmen
z. B.	zum Beispiel
z. T.	zum Teil
v.a.	vor allem
vgl.	vergleiche

1.2 Rechtstexte

AO	Abgabenordnung in der Fassung der Bekanntmachung vom 23.01.2025
BDSG	Bundesdatenschutzgesetz vom 30.06.2017
DSGVO	Verordnung (EU) 2016/679 (Datenschutzgrundverordnung) vom 27.04.2016
OZG	Onlinezugangsgesetz vom 14.08.2017
OZG-SV	Standardverordnung Onlinezugang vom 23.09.2025
SGB X	Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18.01.2001

in der jeweils aktuellen Fassung

2 Einleitung

2.1 Inhalt

Der standardisierte Prüfprozess bietet eine strukturierte Handlungsanleitung zur Umsetzung der **Vorgaben der DSGVO** und der **datenschutzrechtlichen Spezialnormen** bei der Entwicklung oder grundlegenden Überarbeitung von länderübergreifenden Onlinediensten i. S. d. §§ 2 Abs. 8, 8a OZG, mit denen das Nachnutzungsmodell „Einer-für-Alle“ umgesetzt wird (**„EfA-Onlinedienste“**).

EfA-Onlinedienste i. S. d. OZG unterfallen darüber hinaus dem weiteren Begriff der „**Onlineservices**“ und „**Onlineportale**“ i. S. d. **DIN SPEC 66336, 3.15** und **3.16**, so dass insbesondere die Vorgaben zum Datenschutz nach **DIN SPEC 66336, 5.8** berücksichtigt und konkretisiert werden. Sofern die Anforderungen der DIN SPEC 66336 eingehalten werden, enthält die Verordnung des Bundesministeriums für Digitales und Staatsmodernisierung über Standards für den Onlinezugang zu Verwaltungsleistungen (OZG-SV) in § 2 Abs. 2 die Vermutung, dass die allgemein anerkannten Regeln der Technik im Sinne der Verordnung eingehalten werden.

Darüber hinaus greift der standardisierte Prozess insbesondere zur Bestimmung der verschiedenen Rollen, auf die verbindlichen **Mindestanforderungen an den Betrieb von „Einer für Alle“-Services des IT-Planungsrates** zurück.

2.2 Anwendende

Der standardisierte Prüfprozess richtet sich in erster Linie an die Behörden, die **EfA-Onlinedienste i. S. d. OZG** betreiben und denen damit die datenschutzrechtliche Verantwortung zugewiesen ist (siehe dazu **Standardprozessschritt 2 und 3**).

Entsprechend des weiten Anwendungsbereichs der DIN SPEC 66336 richtet sich der Prüfprozess aber auch an weitere an der Umsetzung von EfA-Onlinediensten i. S. d. OZG beteiligte Stellen (**Umsetzende**, **Steuernde** und **Prüfende**, siehe **DIN SPEC 66336, Einleitung**).

Der Prüfprozess kommt zudem insbesondere bei der **Neuentwicklung** oder bei der **grundlegenden Überarbeitung** eines EfA-Onlinedienstes i. S. d. OZG zur Anwendung (vgl. Anwendungsbereich **DIN SPEC 66336, 1.**).

2.3 Methodik

Der standardisierte Prüfprozess orientiert sich an den klassischen **Phasen des Projektmanagements**, die in Bund und Ländern durch verschiedene Instrumente z. T. verbindlich vorgegeben werden (siehe v.a. **DIN 69901**, **Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung der Bundesregierung** sowie Projektmanagementhandbücher auf Landesebene, vgl. **Anlage 8.2.1**).

Zu den klassischen Phasen des Projektmanagements zählen:

1. Initialisierungsphase
2. Definitionsphase
3. Planungsphase
4. Durchführungsphase
5. Abschlussphase

Jeder Projektmanagementphase ordnet der Prüfprozess **Standardprozessschritte** zu. Bei den Standardprozessschritten handelt es sich um die wichtigsten Fragen, die aus datenschutzrechtlicher Sicht zu prüfen und zu klären sind.

Anlage 8.1 enthält unter Berücksichtigung aller Standardprozessschritte einen Vorschlag einer **Standardstruktur für** ein **Datenschutzkonzept mit anschließender Datenschutz-Folgenabschätzung**.

2.4 Aufbau

Der standardisierte Prüfprozess bietet im Folgenden zunächst eine Übersicht, mittels derer auf einen Blick erkennbar ist, in welcher Projektmanagementphase welcher Standardprozessschritt bearbeitet werden sollte.

Die sich anschließenden Abschnitte widmen sich den einzelnen Projektmanagementphasen. Dort wird jeweils beispielhaft in Anlehnung an den **Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung der Bundesregierung** mittels Schaubild dargestellt, welche Arbeitsschritte diese Phase aus Sicht des Projektmanagements umfasst. Der Kerninhalt dieser Phase wird zusammengefasst und es wird herausgearbeitet, an welchen Arbeitsschritten datenschutzrechtliche Fragestellungen mitberücksichtigt werden sollten. Die betroffenen Arbeitsschritte werden jeweils im Schaubild farblich hervorgehoben. Im Anschluss werden die für die einzelnen Projektmanagementphasen konkreten datenschutzrechtlichen Standardprozessschritte beschrieben und die Bezüge zu Punkt 5.8 DIN SPEC 66336 aufgezeigt.

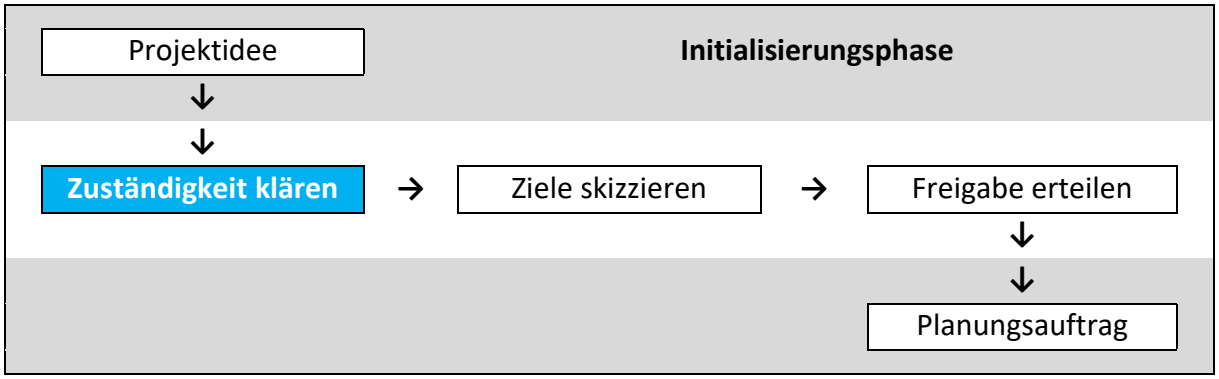
Die Anlagen enthalten ergänzende Hilfestellungen für die Umsetzung der datenschutzrechtlichen Anforderungen.

3 Übersicht der Standardprozessschritte (SPS) entlang der Projektmanagementphasen

Initialisierung	Definition	Planung	Durchführung	Abschluss
Onlinedienst i. S. d. OZG? SPS 1	Welche personenbezogenen Daten werden verarbeitet? SPS 6	Data Protection by Design Art. 25 DSGVO SPS 12		Datenschutz-Management SPS 17
Betreibende Behörde? SPS 2	Modellierung nach Standard-Datenschutz-Modell (SDM) SPS 7	Schwellwertanalyse SPS 13		
Verantwortung i. S. d. DSGVO? SPS 3	Rechtsgrundlagen § 8a Abs. 1 OZG SPS 8	Bestimmung der technischen und organisatorischen Maßnahmen (TOMs) unabhängig vom Risiko SPS 14		
Auftragsverarbeitende? SPS 4	Löschung der personenbezogenen Daten § 8a Abs. 3 OZG SPS 9	gegebenenfalls Datenschutz-Folgenabschätzung (DSFA) SPS 15		
Unter-Auftragsverarbeitende? SPS5	Gewährleistung der Betroffenenrechte SPS 10	Dokumentation in Verzeichnis von Verarbeitungstätigkeiten / Datenschutzkonzept / Datenschutz-Folgenabschätzung SPS 16		
	Risiko-Vorprüfung SPS 11			

4 Initialisierungsphase

4.1 Prüfungsschritte im Rahmen der Initialisierungsphase



Im Rahmen der Initialisierungsphase wird eine grobe Vorstellung über die Zielsetzungen des Projektes entwickelt und es werden erste **Zuständigkeiten und** die **Verantwortung** geklärt. Je nach Umfang des Projektes kann die Initialisierungsphase mit der nachfolgenden Definitionsphase zusammenfallen, sofern die Ziele bereits hinreichend skizziert sind (siehe Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung, S. 14 f.). Bereits im Rahmen dieser Frühphase der Entwicklung sollten aus Sicht des Datenschutzes die nachfolgenden Standardprozessschritte 1 bis 5 geklärt werden.

Beachte zum Begriff der Verantwortung/ Verantwortlichkeit:

- Im Bereich des **Datenschutzes** ist der enge Begriff der Verantwortlichkeit i. S. d. **Art. 4 Nr. 7 DSGVO** maßgeblich.
- Das **Projektmanagement** geht vom weiteren Begriff der **Projektverantwortung/ -zuständigkeit** aus (s.o.).
- Die **DIN SPEC 66336, 3.30** nutzt hinsichtlich der Projektverantwortung den Begriff **„steuernde Stelle“**.
- Die **Mindestanforderungen an den Betrieb von „Einer für Alle“-Services** nutzen den Begriff **„Betriebsverantwortlichkeit“**.

4.2 Zu prüfende Fragen im Rahmen der Initialisierungsphase

Standardprozessschritt 1: Liegt ein EfA-Onlinedienst i. S. d. OZG vor?

Ausgangspunkt ist die genaue Definition des Begriffs „länderübergreifende Onlinedienste“ in § 2 Abs. 8 OZG.

In Zweifelsfällen sollten die detaillierten Erläuterungen in der Orientierungshilfe der Datenschutzkonferenz zu ausgewählten Fragestellungen des neuen Onlinezugangsgesetzes berücksichtigt werden.

Bestehen weiterhin Zweifel, ob ein Onlinedienst i. S. d. OZG vorliegt, sollte die für die datenschutzrechtliche Begleitung des Projektes zuständige Stelle oder Person bzw. die oder der behördliche Datenschutzbeauftragte bzw. die zuständige Datenschutzaufsichtsbehörde um Beratung gebeten werden.

Standardprozessschritt 2: Wer ist betreibende Behörde?

Gemeint ist hier die den **Onlinedienst betreibende Behörde i. S. d. § 8a Abs. 4 OZG**, die nach dieser Norm als Verantwortliche i. S. d. Datenschutzes einzustufen ist (siehe nächster **Standardprozessschritt 3**).

Im Regelfall sollte die den Onlinedienst betreibende Behörde i. S. d. OZG der **Rolle 3 „Betriebsverantwortlicher“** nach den **Mindestanforderungen an den Betrieb von „Einer für Alle“-Services** sowie der Rolle **„steuernde Stelle“** nach **DIN SPEC 66336, 3.30**, die auch nach DIN SPEC 66336, 5.3.1 für den Datenschutz verantwortlich sein soll, entsprechen. Auf diese Standards kann gegebenenfalls zu Auslegungszwecken zurückgegriffen werden.

In der Praxis ist die Betriebsverantwortung für die EfA-Onlinedienste i. S. d. OZG regelmäßig der für Verwaltungsdigitalisierung oder fachlich zuständigen Hauptverwaltung zugewiesen.

Hiervon zu unterscheiden ist der rein **technische Betrieb** des Onlinedienstes, der regelmäßig durch die **(Landes-) IT-Dienstleistenden / Rechenzentren** erfolgt (entspricht **Rolle 4 „OD Bereitsteller/ Second Level Support (technisch)“** nach **Mindestanforderungen an den Betrieb von „Einer für Alle“-Services).**

Standardprozessschritt 3: Welche öffentliche Stelle ist Verantwortliche i. S. d. DSGVO?

Die Verantwortlichkeit i. S. d. Art. 4 Nr. 7 DSGVO wird durch **§ 8a Abs. 4 Satz 1 OZG gesetzlich zugewiesen**.

Die unter **Standardprozessschritt 2** als **Betreiberin des EfA-Onlinedienstes** i. S. d. OZG zuständige Stelle ist gemäß § 8a Abs. 4 OZG die **Verantwortliche i. S. d. DSGVO**.

Die datenschutzrechtliche Verantwortlichkeit der Behörde, an die zum Zwecke der Durchführung des Verwaltungsverfahrens personenbezogene Daten übermittelt werden, bleibt im Hinblick auf die Datenverarbeitung im Rahmen des Verwaltungsverfahrens unberührt (**§ 8a Abs. 4 Satz 2 OZG).**

Auf Grund der gesetzlichen Zuweisung der Verantwortlichkeit sind hinsichtlich der Verarbeitung personenbezogener Daten im EfA-Onlinedienst keine Auftragsverarbeitungsverträge i. S. d. Art. 28 DSGVO oder Vereinbarungen zur gemeinsamen Verantwortung i. S. d. Art. 26 Abs. 1 Satz 2 DSGVO mit den Behörden der nachnutzenden Länder abzuschließen!

Standardprozessschritt 4: Welche Auftragsverarbeiter i. S. d. DSGVO kommen zum Einsatz?

Auftragsverarbeiter sind nach den einschlägigen Normen der **Art. 4 Nr. 8 DSGVO und Art. 28 DSGVO** zu bestimmen.

Im Rahmen der Bereitstellung von EfA-Onlinediensten i. S. d. OZG erfolgt typischerweise der technische Betrieb mittels einer Auftragsverarbeitung.

Damit sind im Regelfall beteiligte (Landes-) IT-Dienstleister als Auftragsverarbeiter einzustufen, die nach den Vorgaben des **Art. 28 Abs. 3 DSGVO** im Rahmen eines Auftragsverarbeitungsvertrages (oder eines anderen Rechtsinstruments) zu verpflichten sind. Zentrales Merkmal der Auftragsverarbeitung ist die Weisungsgebundenheit des Auftragsverarbeiters. Auch verbleibt bei Inanspruchnahme eines Auftragsverarbeiters die datenschutzrechtliche Verantwortlichkeit bei der betreibenden Behörde.

Beim Einsatz von (Unter-)Auftragsverarbeitern muss geprüft werden, ob diese im Rahmen der Erbringung ihrer Leistungen personenbezogene Daten außerhalb des Europäischen Wirtschaftsraums verarbeiten. Solche Verarbeitungen sind nur dann zulässig, wenn neben den allgemeinen Vorgaben auch die besonderen Voraussetzungen des Kapitels V DSGVO (Art. 44 – 50 DSGVO) erfüllt werden.

Auch bei einer geplanten Inanspruchnahme von Cloud-Diensten muss sichergestellt werden, dass die Vorgaben der DSGVO uneingeschränkt umgesetzt werden können. Eine Orientierung bietet das Positionspapier der Datenschutzkonferenz „Kriterien für Souveräne Clouds“ vom 11. Mai 2023.

Gegebenenfalls wird in der Initialisierungsphase noch nicht über den Einsatz von Auftragsverarbeitern entschieden, sondern erst im Rahmen der Planungs- oder Durchführungsphase. In diesem Fall ist dieser Standardprozessschritt später (erneut) durchzuführen.

Standardprozessschritt 5: Welche Unter-Auftragsverarbeiter kommen zum Einsatz?

Die den Onlinedienst betreibende Stelle muss als datenschutzrechtlich Verantwortliche sicherstellen, dass nicht nur die eingesetzten Auftragsverarbeiter, sondern auch weitere von diesen eingesetzten Auftragsverarbeiter (**Unter-Auftragsverarbeiter**) datenschutzrechtlich zuverlässig sind (**Art. 28 Abs. 1 DSGVO).**

Grundsätzlich dürfen Auftragsverarbeiter keine weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen einsetzen (**Art. 28 Abs. 2 Satz 1 DSGVO**).

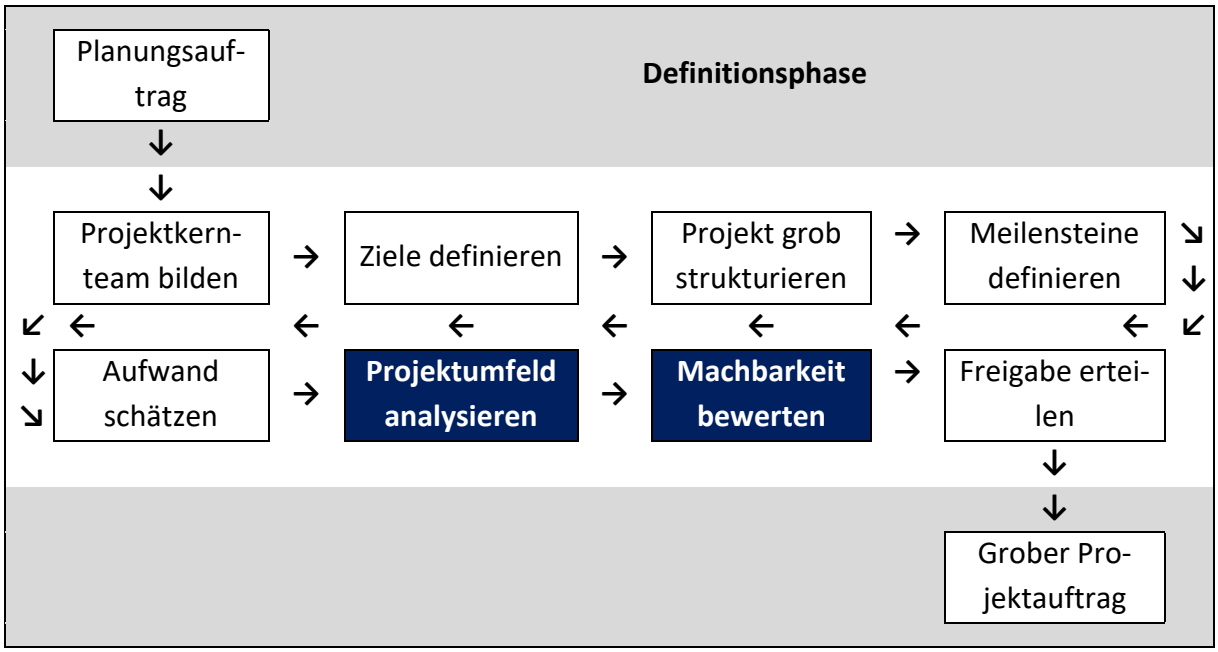
Die betreibende Stelle muss als Verantwortliche:

- die konkreten Bedingungen für die Inanspruchnahme von Unter-Auftragnehmenden im Auftragsverarbeitungsvertrag (AVV) festlegen (**Art. 28 Abs. 3 lit. d DSGVO**);
- durch den Auftragsverarbeiter über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung anderer Auftragsverarbeiter informiert werden (**Art. 28 Abs. 2 Satz 2 DSGVO**).

Wie der Standardprozessschritt 4 muss auch dieser Prozessschritt gegebenenfalls (erneut) in der Planungs- oder Durchführungsphase durchgeführt werden.

5 Definitionsphase

5.1 Prüfungsschritte im Rahmen der Definitionsphase



Ergebnis der Projektdefinition ist die Zusammenstellung entscheidungsrelevanter Informationen in Form eines groben Projektauftrages. Aus ihm geht hervor, welche konkreten Ziele verfolgt werden sollen, welcher Aufwand zur Erreichung dieser Ziele erforderlich ist und welche Bedingungen das Projekt beeinflussen könnten. Darüber hinaus enthält der Projektauftrag eine erste Bewertung der Machbarkeit aus Sicht der Projektleitung (siehe Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung, S. 16 ff.).

Typischerweise werden in der Definitionsphase eine **Projektumfeldanalyse** sowie eine **Machbarkeitsprüfung** durchgeführt, in die sich die **Vorgaben des Datenschutzes als Projektumfeldfaktoren** sinnvoll integrieren lassen. Dies eröffnet die Möglichkeit, die Vorgaben des Datenschutzes möglichst früh in die Projektplanung einzusteuern und so zu verhindern, dass diese zu spät, d. h. erst zum Abschluss der Durchführungsphase oder kurz vor Beginn des Echtbetriebes des Projektes in den Blick geraten.

5.2 Zu prüfende Fragen im Rahmen der Definitionsphase

Standardprozessschritt 6: Welche personenbezogenen Daten werden im Onlinedienst verarbeitet?

Es erfolgt eine präzise Abgrenzung, welche der verarbeiteten Daten als personenbezogene Daten i. S. d. Definition des **Art. 4 Nr. 1 DSGVO** zu bewerten sind. Dabei bedarf es auch einer genauen Bestimmung des Zwecks (Art. 5 Abs. 1 lit. a DSGVO), zu dem die personenbezogenen Daten verarbeitet werden. Im Regelfall werden bei einem länderübergreifenden Onlinedienst i. S. d. OZG personenbezogene Daten in Form von Antragsdaten wie Name, Adresse, Geburtsdatum usw. zu dem in § 8a Abs. 1 S. 1 OZG definierten Zweck der Unterstützung bei der

Inanspruchnahme einer elektronischen Verwaltungsleistung, der Offenlegung der Daten aus dem Online-Formular an die jeweils zuständige Behörde sowie der Übermittlung von elektronischen Dokumenten zu Verwaltungsvorgängen an die Nutzenden verarbeitet. Die Zusammenfassung bestimmter Datentypen zu Gruppen (z. B. Namen, Adresse, Geburtsdatum zu Antragsdaten) reicht nicht aus.

Wichtig ist eine genaue Prüfung und Dokumentation, ob darüber hinaus sensible Daten, wie etwa **„besondere Kategorien personenbezogener Daten" i. S. d. Art. 9 Abs. 1 DSGVO**, personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten i. S. d. **Art. 10 DSGVO**, dem **Steuergeheimnis i. S. d. § 30 AO** unterliegende Daten oder Daten, die nach Übermittlung an die zuständige Behörde als **Sozialdaten i. S. d. § 67 Abs. 2 SGB X** zu qualifizieren sind, verarbeitet werden.

Insgesamt empfiehlt es sich, die bestimmten Datentypen (mindestens) anhand der folgenden Kriterien zu strukturieren:

- „einfache" personenbezogene Daten, **Art. 4 Nr. 1 DSGVO**
- besondere Kategorien personenbezogener Daten, **Art. 9 Abs. 1 DSGVO**
- personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten, **Art. 10 DSGVO**
- Sozialdaten i. S. d. **§ 67 Abs. 2 SGB X**
- dem **Steuergeheimnis i. S. d. § 30 AO** unterliegende Daten

Darüber hinaus sollte aber auch bei „einfachen" personenbezogene Daten stets geprüft werden, ob diese im Einzelfall, z. B. aufgrund des Verwendungskontextes, ihrer Verkettbarkeit oder ihres quantitativen Umfangs einen ähnlich hohen Schutzbedarf wie die genannten Datentypen aufweisen.

Standardprozessschritt 7: Wie werden die personenbezogenen Daten verarbeitet?

Punkt 5.8.3. DIN SPEC 66336 - Datenminimierung

Anschließend an die Prüfung, **welche** personenbezogene Daten verarbeitet werden, muss geprüft und dokumentiert werden, **wie** diese verarbeitet werden. Dies ist insbesondere als Grundlage für die Prüfung der dabei entstehenden Risiken und Auswahl geeigneter Abhilfemaßnahmen (technisch und organisatorische Maßnahmen, TOMs) erforderlich und sollte daher, soweit wie möglich, bereits in der Projektumfeldanalyse und Machbarkeitsprüfung der Definitionsphase berücksichtigt werden. Gegebenenfalls ist dieser Schritt in der Prüfungs- und Durchführungsphase (erneut) durchzuführen. Dieser Schritt fördert zudem auch die Umsetzung des durch die DIN SPEC 66336 vorgegebenen Grundsatzes der Datenminimierung.

Die Verarbeitungstätigkeit im Onlinedienst sollte nach den etablierten **Modellierungstechniken** des **SDM, Teil D.2** beschrieben werden:

SDM Modellierungstechniken
1. Modellierung der Verarbeitungsvorgänge/ -phasen, SDM Teil D.2.1
2. Modellierung der Ebenen des Verfahrens/ der Verarbeitungstätigkeit, SDM Teil D.2.3
3. Modellierung der Komponenten, SDM Teil D.2.5
4. Modellierung als „SDM-Würfel“, SDM, Teil D.2.6

Standardprozessschritt 8: Dürfen die personenbezogenen Daten im Onlinedienst verarbeitet werden?

Punkt 5.8.3. DIN SPEC 66336 - Datenminimierung

Im Regelfall sind EfA-Onlinedienste i. S. d. OZG als sog. **Antragsassistenten** ausgestaltet, d. h. es werden nur personenbezogenen Daten zur Antragsstellung für ein **nachgelagertes Fachverfahren** verarbeitet. Getrennt davon ist die Verarbeitung personenbezogener Daten in diesen nachgelagerten Fachverfahren zu betrachten, die auf Grundlage der im jeweiligen Fachrecht geregelten Rechtsgrundlagen zulässig ist (vgl. z. B. §§ 67a ff. SGB X).

Die den Fachverfahren vorgelagerte Verarbeitung personenbezogener Daten in den EfA-Onlinediensten i. S. d. § 2 Abs. 8 OZG erfolgt demgegenüber auf den **spezialgesetzlichen Rechtsgrundlagen** des **§ 8a Abs. 1 und 2 OZG**, die jeweils einen Erlaubnistatbestand i. S. d. **Art. 6 Abs. 1 lit. e DSGVO** darstellen.

Die einen länderübergreifenden Onlinedienst **betreibende Behörde** (siehe unter **Standardprozessschritt 2**) darf nach **§ 8a Abs. 1 Satz 1 OZG die erforderlichen** personenbezogenen Daten im Onlinedienst verarbeiten für:

1. **die Zwecke der Unterstützung bei der Inanspruchnahme einer elektronischen Verwaltungsleistung**
2. **die Offenlegung der Daten aus dem Online-Formular an die jeweils zuständige Behörde**
3. **die Übermittlung von elektronischen Dokumenten zu Verwaltungsvorgängen an den Nutzer**

§ 8a Abs. 1 Satz 2 OZG erlaubt diese Verarbeitung darüber hinaus auch hinsichtlich **besonderer Kategorien personenbezogener Daten** i. S. d. **Art. 9 Abs. 1 DSGVO**, soweit diese für das an den länderübergreifenden Onlinedienst angeschlossene Verwaltungsverfahren erforderlich sind. § 8a Abs. 1 Satz 2 OZG bildet damit einen Ausnahmetatbestand i. S. d. Art. 9 Abs. 2 DSGVO.

Bei der Verarbeitung von besonderen Kategorien personenbezogener Daten im Onlinedienst ist gemäß **§ 8a Abs. 1 Satz 3 OZG** zudem **§ 22 Abs. 2 BDSG** anzuwenden (siehe dazu **Standardprozessschritt 14**).

Dieser Schritt fördert dabei auch die Umsetzung des durch die DIN SPEC 66336 vorgegebenen Grundsatzes der Datenminimierung.

Standardprozessschritt 9: Wann müssen die personenbezogenen Daten gelöscht werden?

Punkt 5.8.3. und 5.8.6. DIN SPEC 66336 – Datenminimierung; Aufbewahrungsfristen festlegen; fristgerechte Löschung personenbezogener Daten

Es ist ein Löschkonzept für den Onlinedienst i. S. d. OZG zu erstellen. Dabei sind die folgenden Grundsätze und Normen zu beachten:

1. Grundsätzlich dürfen personenbezogene Daten nur solange verarbeitet werden, wie dies für den ursprünglichen Zweck ihrer Verarbeitung erforderlich ist (**Art. 5 Abs. 1 lit. b und e DSGVO** „Zweckbindung“, „Speicherbegrenzung“).

   Grundsätzlich müssen damit alle personenbezogenen Daten im Onlinedienst gelöscht werden, sobald die in § 8a Abs. 1 OZG genannten Verarbeitungszwecke (siehe unter 8.) erfüllt sind.

2. **§ 8a Abs. 2 Satz 1 OZG** gestattet aber, dass die personenbezogenen Daten im länderübergreifenden Onlinedienst **zwischengespeichert** werden dürfen, um dem Nutzer die Möglichkeit zu bieten, das **Online-Formular zu einem späteren Zeitpunkt zu vervollständigen, zu korrigieren oder zu löschen**.

3. **§ 8a Abs. 3 OZG** enthält zudem **konkrete Löschfristen**:

   - **§ 8a Abs. 3 Satz 1 bis 2 OZG**: Die zwischengespeicherten Daten sind in der Regel nach Ablauf von 30 Tagen nach der letzten Bearbeitung des Online-Formulars durch die Nutzerin und den Nutzer automatisch zu löschen. Die Nutzenden sind über die automatische Löschung der zwischengespeicherten Daten zu dem Online-Formular vorab zu informieren.
   - **§ 8a Abs. 3 Satz 3 bis 5 OZG**: Die **längerfristige Speicherung** von Daten im länderübergreifenden Onlinedienst ist **ausnahmsweise zulässig**, wenn *„zu erwarten ist, dass dies für die Unterstützung des Nutzers bei der Inanspruchnahme einer elektronischen Verwaltungsleistung erforderlich ist“*. In solchen Fällen ist eine **angemessene Löschfrist festzulegen**. Die Nutzenden sind über diese Löschfrist zu informieren.

Dieser Schritt fördert dabei im Ergebnis auch die Umsetzung des durch die DIN SPEC 66336 vorgegebenen Grundsatzes der Datenminimierung.

Standardprozessschritt 10: Wie werden die Betroffenenrechte umgesetzt?

Punkt 5.8.5. DIN SPEC 66336 – transparente Information über Verarbeitungen und Schnittstellen; Betroffenenrechte sicherstellen

Bereits im Rahmen der **Projektumfeldanalyse/ Machbarkeitsprüfung** muss die den Onlinedienst betreibende Behörde prüfen, wie sie die Betroffenenrechte der Art. 12 ff. DSGVO hinsichtlich der im Onlinedienst verarbeiteten personenbezogenen Daten gewährleisten kann.

Zu den **Betroffenenrechten** gehören:

- **Informationspflicht** bei Erhebung personenbezogener Daten einer Person bei der Person selbst (**Art. 13 DSGVO**) bzw. bei Dritten (**Art. 14 DSGVO**)
- **Auskunftsrecht** (**Art. 15 DSGVO**)
- Recht auf **Berichtigung** (**Art. 16 DSGVO**)
- Recht auf **Löschung** (**Art. 17 DSGVO**)
- Recht auf **Einschränkung der Verarbeitung** (**Art. 18 DSGVO**)
- **Widerspruchsrecht** (**Art. 21 DSGVO**)

Für die Umsetzung der Betroffenenrechte sind insbesondere die Vorgaben des **Art. 12 DSGVO** zu Fristen, Art und Weise zu beachten.

Besonderes Augenmerk sollte auf die **Datenschutzerklärung gelegt werden**, die den betroffenen Personen vorab zur Verfügung gestellt wird. Informationspflichten können gegebenenfalls entfallen, wenn und soweit die betroffene Person bereits über die Informationen verfügt (**Art. 13 Abs. 4 DSGVO** und **Art. 14 Abs. 5 DSGVO**).

Die Gewährleistung der Betroffenenrechte sollte in einem **Konzept für die Umsetzung der Betroffenenrechte für den Onlinedienst i. S. d. OZG** geplant und dokumentiert werden.

Insbesondere mit Blick auf die **länderübergreifende Struktur der Onlinedienste i. S. d. OZG** müssen die betreibenden Behörden sicherstellen, dass

- die betroffenen Personen besonders sorgfältig über die länderübergreifende Verarbeitung ihrer Daten im Rahmen des Onlinedienstes aufgeklärt werden (z. B. durch eine gut verständliche Datenschutzerklärung, die eine Aufklärung über die Betroffenenrechte sowie eine Benennung der für das nachgelagerte Verwaltungsverfahren verantwortlichen Behörde enthält);

- die betroffenen Personen genau über die Anlaufstellen in den verschiedenen Bundesländern informiert werden, an die sie sich zur Realisierung Ihrer Rechte aus der DSGVO richten können.

Standardprozessschritt 11: Entsteht voraussichtlich ein hohes Risiko aus Sicht des Datenschutzes? („Risiko-Vorprüfung“)

Bereits in der **Projektumfeldanalyse und Machbarkeitsprüfung** muss geprüft werden, ob voraussichtlich ein hohes Risiko aus Sicht des Datenschutzes entsteht. Im Unterschied zum Standardprozessschritt 13 findet hier eine Vorprüfung anhand der zu diesem Projektzeitpunkt bekannten Umstände statt.

Führt die im Onlinedienst geplante Verarbeitung personenbezogener Daten zu einem **hohen Risiko (Art. 35 Abs. 1 DSGVO)**, so entsteht ein besonderer Prüfungsaufwand hinsichtlich der Risiken und erforderlichen TOMs (**Datenschutz-Folgenabschätzung, siehe Standardprozessschritte 13. bis 15.**). Abschließend wird dies im Rahmen der **„Schwellwertanalyse“** (siehe unter **Standardprozessschritt 13**) geprüft. Anhand der anerkannten Regelbeispiele, die keinen gesonderten Prüfungsaufwand erfordern, kann das Projektteam bereits früh ein hohes Datenschutzrisiko erkennen:

1. **Entspricht die geplante Verarbeitung personenbezogener Daten im Onlinedienst einem der Verarbeitungsvorgänge der „Muss-Liste“ der zuständigen Aufsichtsbehörde (Art. 35 Abs. 4 DSGVO)?**

   z. B.: umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 DSGVO und Art. 10 DSGVO handelt (siehe **Anlage 8.2.2**)

2. **Entspricht die geplante Verarbeitung personenbezogener Daten im Onlinedienst dem Regelbeispiel des Art. 35 Abs. 3 lit. b DSGVO** („Umfangreiche Verarbeitung von personenbezogenen Daten gemäß Art. 9 Abs. 1 und 10 DSGVO“)?

3. **Liegt ein Fall der Liste des EDSA, Working Paper 248, rev. 01 vor?**

Erfüllt die geplante Verarbeitung im Onlinedienst zwei oder mehr der Kriterien des **Working Paper 248, rev. 01**, so soll im Regelfall ein hohes Risiko i. S. d. Art. 35 DSGVO vorliegen.[1] Diese Kriterien sind:

- Bewerten oder Einstufen (Scoring) („Evaluation or scoring“)

[1] Siehe EDSA, 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“ vom 4. April 2017, S. 10 f.

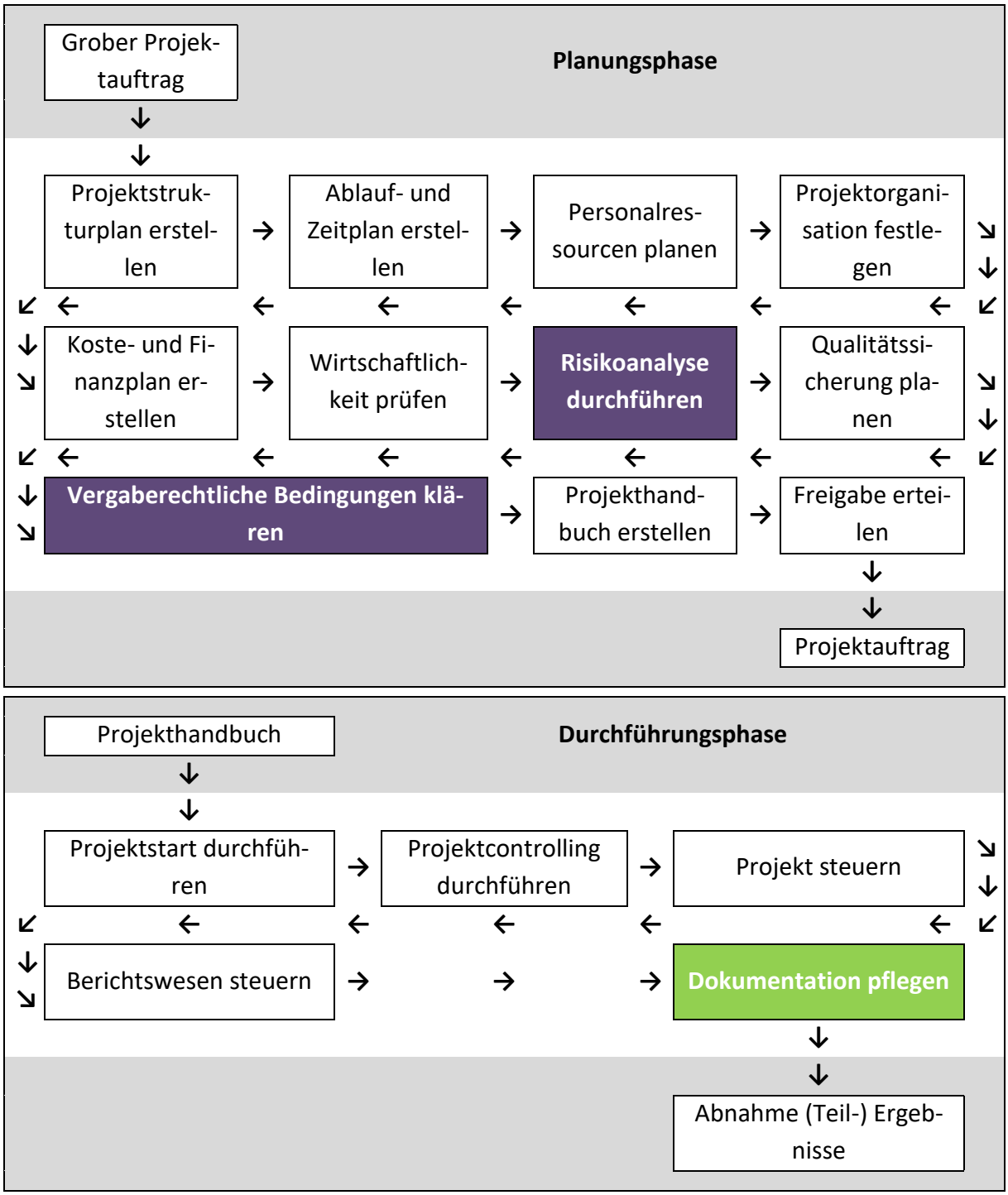
- Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung („Automated-decicion making with legal or similar significant effect“)
- Systematische Überwachung („Systematic monitoring“)
- Vertrauliche Daten oder höchst persönliche Daten („Sensitive data or data of a highly personal nature“)
- Datenverarbeitung in großem Umfang („Data processed in a large scale“)
- Abgleichen oder Zusammenführen von Datensätzen („Matching or combining datasets“)
- Daten zu schutzbedürftigen Betroffenen (Data concerning vulnerable data subjects“)
- Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen („Innovative use or applying new technological or organisational solutions“)
- Betroffene werden an der Ausübung ihres Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages gehindert („When the processing in itself prevents data subjects from exercising a right or using a service or a contract“)

Die möglichst frühe Ermittlung des Datenschutzrisikos erlaubt zudem ein abgestimmtes Vorgehen zwischen technisch-organisatorischem Datenschutz und Informationssicherheit unter Realisierung von wertvollen Synergiepotenzialen. So ermöglichen es beispielsweise die ermittelten maximalen datenschutzrechtlichen Ausgangsrisiken, datenschutzrechtliche Erkenntnisse zeitgerecht in die Schutzbedarfsfeststellung der Informationssicherheit (nach IT-Grundschutz des BSI[2]) einzubringen.

[2] Siehe BSI - IT-Grundschutz, unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html.

6 Planungs- und Durchführungsphase

6.1 Prüfungsschritte im Rahmen der Planungs- und Durchführungsphase



Im Verlauf der Planungsphase wird typischerweise eine **Risikoanalyse** (auch „Chancen- und Risikomanagement“) durchgeführt. Aufgabe der Risikoanalyse ist es, die den Projekterfolg gefährdenden Faktoren (hinsichtlich Leistung, Kosten und Termine) zu identifizieren, mittels definierter Kriterien zu bewerten, in einem Risikoportfolio abzubilden und gegebenenfalls entsprechende Gegenmaßnahmen festzulegen (siehe Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung, S. 34 f.).

Auch aus Sicht des Datenschutzes ist eine Analyse durchzuführen, inwieweit die geplante **Verarbeitung personenbezogener Daten zu Risiken für die betroffenen Personen** führt. Diese lässt sich sinnvoll anhand der nachfolgenden **Standardprozessschritte 12 bis 15**, unter Beachtung der besonderen Anforderungen der DSGVO, als Teil der allgemeinen Risikoanalyse des Projektmanagements ausgestalten.

Grundlage der **Risikoanalyse aus Sicht des Datenschutzes** sind stets die tatsächlichen Datenverarbeitungstätigkeiten, die mit der konkreten technischen Umsetzung des Projektes oft erst im Verlauf der **Durchführungsphase** abschließend festgelegt werden. Die nachfolgenden Prüfpunkte müssen daher, soweit erforderlich, in die Durchführungsphase verlagert bzw. mehrfach durchlaufen werden.

Soweit der **Entwicklungsprozess** des Onlinedienstes in dieser Phase des Projektes nach den klassischen **Phasen des Lebenszyklus eines digitalen Produktes** (Analyse, Umsetzung, Betrieb und Weiterentwicklung, siehe **DIN SPEC 66336, 4.**) strukturiert ist, sollten die **Standardprozessschritte 12 bis 15**, gegebenenfalls mehrfach, in diesen Phasen durchlaufen werden.

6.2 Zu prüfende Fragen im Rahmen der Planungs- und Durchführungsphase

Standardprozessschritt 12: Wie werden die Vorgaben des Art. 25 DSGVO erfüllt?

Punkt 5.8.4. DIN SPEC 66336 – „Datenschutz durch Technikgestaltung" und „datenschutzfreundliche Voreinstellungen" umsetzen

Bestehende und zu entwickelnde Onlinedienste i. S. d. OZG müssen die Vorgaben des **Art. 25 DSGVO** („Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen") umsetzen.

Die rechtliche Verpflichtung des Art. 25 DSGVO bindet jedoch zunächst nur die den Onlinedienst betreibende Behörde und gegebenenfalls ihre Auftragsverarbeiter – nicht „automatisch" gebunden sind einbezogene **Hersteller:innen/ Entwickler:innen**. Diese müssen durch entsprechende Vergabe- und Vertragsbedingungen verpflichtet werden.

Sofern ein Vergabeverfahren durchzuführen ist, sollte die betreibende Behörde bereits in der **Planungsphase** (als dem Zeitpunkt der Festlegung der Verarbeitungsmittel i. S. d. Art. 25 Abs. 1 DSGVO) die Vorgaben des Art. 25 DSGVO in die **vergaberechtlichen Bedingungen** integrieren. Auf dieser Grundlage können sodann die Unterlagen für das Vergabeverfahren erstellt werden, insbesondere in Form der Leistungsbeschreibung.

Standardprozessschritt 13: Entsteht ein hohes Risiko aus Sicht des Datenschutzes? („Schwellwertanalyse")

Die Vorgaben des technischen Datenschutzes verpflichten die betreibende Behörde und ihre Auftragsverarbeiter insbesondere dazu, **geeignete technische und organisatorische**

Maßnahmen (TOMs) zur Gewährleistung eines **angemessenen Schutzniveaus** umzusetzen **(Art. 32 DSGVO)**.

Die Auswahl der zu ergreifenden TOMs hat dabei unter Berücksichtigung des **Stands der Technik**,[3] der **Implementierungskosten** und der Art, des Umfangs, der Umstände und der **Zwecke der Verarbeitung** sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des **Risikos für die Rechte und Freiheiten der betroffenen Personen** zu erfolgen. Dabei ist zu beachten, dass die nach Art. 32 Abs. 1 DSGVO geforderte Berücksichtigung des **„Stands der Technik"** nicht bereits durch Einhaltung der **„allgemein anerkannten Regeln der Technik"** erfüllt ist, die gem. § 2 Abs. 2 OZG-Standardverordnung[4] bei Erfüllung der Anforderungen der DIN SPEC 66336 vermutet wird.

Hinsichtlich des **Risikos für die Rechte und Freiheiten der betroffenen Personen** unterscheidet die DSGVO im Ergebnis zwischen einem **geringen/ einfachen Risiko** und einem **hohen Risiko** (vgl. **Erwägungsgrund 76 DSGVO**). Da es vollständig risikolose Verarbeitungen nicht geben kann, wird die Formulierung „nicht zu einem Risiko" von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko" führend verstanden. Es empfiehlt sich für die Praxis, zunächst zu prüfen, inwieweit die Verarbeitung personenbezogener Daten im Onlinedienst zu einem **hohen Risiko i. S. d. Art. 35 DSGVO führt („Schwellwertanalyse"),** da nur dann eine strukturierte Risikoanalyse in Form einer **Datenschutz-Folgenabschätzung (DSFA)** durchzuführen ist (siehe **Standardprozessschritt 15**).

Für die **Schwellwertanalyse i. S. d. Art. 35 DSGVO**, d.h. um zu eruieren, ob ein hohes Risiko für die Verarbeitung personenbezogener Daten besteht und aufgrund dessen in der Folge für die betroffenen Datenverarbeitungen zwingend eine DSFA durchzuführen ist, sollte wie folgt vorgegangen werden:

1. **Liegt ein Fall der „Muss-Liste" der zuständigen Aufsichtsbehörde von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO vor?**

   Die Aufsichtsbehörden veröffentlichen Listen mit Verarbeitungstätigkeiten, bei denen pauschal von einem hohen Risiko i. S. d. Art. 35 Abs. 1 DSGVO ausgegangen werden kann (vgl. **Anlage 8.2.2**).

2. **Besteht eine gesetzliche Pflicht zur Erstellung einer DSFA nach Art. 35 Abs. 3 DSGVO?**

   Besonders praxisrelevant für Onlinedienste i. S. d. DSVGO dürfte das Regelbeispiel nach **Art. 35 Abs. 3 lit. b DSGVO („umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten i. S. d. Art. 9 DSGVO und Art. 10 DSGVO")** sein.

[3] Siehe zum Begriff des „Stands der Technik" EDSA „Leitlinien 4/2019 zu Artikel 25 Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen", Version 2.0 vom 20. Oktober 2020, Rn. 18 ff.
[4] Siehe Verordnung über Standards für den Onlinezugang zu Verwaltungsleistungen (OZSV) vom 22. September 2025, BGBl. 2025 I Nr. 221 vom 25. September 2025.

3. **Liegt ein Fall der Liste des EDSA, Working Paper 248, rev. 01 vor?**

   Erfüllt die Verarbeitung im Onlinedienst zwei oder mehr der Kriterien des **Working Paper 248, rev. 01**, so soll im Regelfall ein hohes Risiko i. S. d. Art. 35 DSGVO vorliegen.[5] (siehe Liste der Kriterien unter Standardprozessschritt 11).

4. **Besteht aus sonstigen Gründen im konkreten Fall ein hohes Risiko?**

   Auch wenn im Rahmen der Fragen 1. bis 3. noch kein hohes Risiko festgestellt wurde, muss unter Betrachtung aller Umstände des Einzelfalls geprüft werden, ob die Verarbeitung im Onlinedienst zu einem hohen Risiko führt (siehe Methodik des **DSK Kurzpapiers Nr. 18**).

5. **Ergebnis**

➔ **einfaches/geringes Risiko: weiter mit Standardprozessschritt 14**
➔ **hohes Risiko: weiter mit Standardprozessschritten 14 und 15**

Beachte: Jede Verarbeitung personenbezogener Daten stellt einen Eingriff in das Recht auf Schutz der personenbezogenen Daten bzw. auf informationelle Selbstbestimmung dar und führt damit mindestens zu einem einfachen/ geringen Risiko. Eine vollständig risikolose Verarbeitung kann es damit nicht geben (siehe DSK-Kurzpapier Nr. 18, S. 2), so dass immer mindestens Standardprozessschritt 14 zu durchlaufen ist, wenn nicht Standardprozessschritt 15 anzuwenden ist. Auch ist es denkbar, dass verschiedene Datenverarbeitungsvorgänge durchgeführt werden, hinsichtlich der einerseits Standardprozessschritt 14 und andererseits Standardprozessschritt 15 zu durchlaufen sind.

Beachte: Im Unterschied zum allgemeinen Risikomanagement und auch zum Risikomanagement in der Informationssicherheit besteht **im Bereich des Datenschutzes** grundsätzlich die **Pflicht**, die durch die Verarbeitung personenbezogener Daten entstehenden **Risiken** mit geeigneten und angemessenen technischen und organisatorischen Maßnahmen auf ein angemessenes Schutzniveau **zu reduzieren**. Risiken können daher nicht im selben Maß „in Kauf genommen" werden. So **stehen** die aus dem Bereich der Informationssicherheit bekannten Instrumente der **Risikoakzeptanz** oder des **Risikotransfers** der verantwortlichen Stelle **nur in sehr begrenztem Umfang zur Verfügung** (vgl. **SDM, Teil D.3.1**).

[5] Siehe EDSA, 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" vom 4. April 2017, S. 10 f.

Standardprozessschritt 14: Welche technischen und organisatorischen Maßnahmen (TOMs) sind bei einem einfachen/geringen Risiko umzusetzen?

Punkt 5.8.2 DIN SPEC 66336 – geeignete TOMs festlegen zur angemessenen Minderung der mit der Verarbeitung personenbezogener Daten einhergehenden Risiken

Standardprozessschritt 14 ist hinsichtlich aller Datenverarbeitungsvorgänge durchzuführen, hinsichtlich der **in Standardprozessschritt 13 kein hohes Risiko** i. S. d. Art. 35 DSGVO festgestellt wurde.

Auch bei einfachen/ geringen Risiken müssen Verantwortliche und Auftragsverarbeiter ein angemessenes Schutzniveau durch geeignete TOMs gewährleisten (siehe insbesondere **Art. 32 DSGVO**). Anschließend an die Prüfung nach Standardprozessschritt 13 sind dazu das (einfache) Risiko einer Verletzung des Schutzes der Rechte und Freiheiten natürlicher Personen sowie deren mögliche Folgen zu ermitteln, wobei die Bewertung grundsätzlich unter Berücksichtigung der Eintrittswahrscheinlichkeit und der Schwere der Risiken erfolgen muss. Darüber hinaus ist zu prüfen, ob die umgesetzten TOMs, insbesondere unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, die Risiken ausreichend abmildern und somit angemessen sind.

Unabhängig vom Ergebnis der Schwellwertanalyse sind bei einer **Verarbeitung und Zwischenspeicherung von besonderen Kategorien personenbezogener Daten i. S. d. Art. 9 Abs. 1 DSGVO** im Onlinedienst stets die Vorgaben des **§ 22 Abs. 2 BDSG** umzusetzen (vgl. § 8a Abs. 1 Satz 3 OZG und § 8a Abs. 2 Satz 2 OZG). § 22 Abs. 2 BDSG ergänzt dabei die bereits in Art. 32 Abs. 1 DSGVO genannten konkreten spezifischen Maßnahmen. Personenbezogene Daten i. S. d. Art. 9 Abs. 1 DSGVO, die in einem Onlinedienst verarbeitet und insbesondere länger gespeichert werden, sollten danach stets mindestens nach aktuellem Stand der Technik **verschlüsselt** werden (siehe Art. 32 Abs. 1 lit. a DSGVO, § 22 Abs. 2 Nr. 7 BDSG).

Bei der Bewertung einfacher und geringer Risiken sowie bei der Identifikation geeigneter TOMs lassen sich darüber hinaus auch die Generischen Maßnahmen des Standard-Datenschutz-Modells (**SDM**) (Teil D.1) als Orientierung heranziehen.

Ergänzend können hier auch einzelne oder mehrere der **SDM Bausteine** herangezogen werden:

Baustein 11 „Aufbewahren“ **Baustein 41 „Planen und Spezifizieren“** **Baustein 42 „Dokumentieren“**	**Baustein 51 „Zugriffe auf Daten, Systeme und Prozesse regeln“** **Baustein 60 „Löschen und Vernichten“** **Baustein 61 „Berichtigen“**

Baustein 43 „Protokollieren“ **Baustein 50 „Trennen“**	**Baustein 62 „Einschränken der Verarbeitung“**

Standardprozessschritt 15: Welche TOMs sind bei einem hohen Risiko umzusetzen? (Datenschutz-Folgenabschätzung)

Punkt 5.8.1 DIN SPEC 66336 –Datenschutz-Folgenabschätzung erstellen

Standardprozessschritt 15 ist nur durchzuführen, wenn in Standardprozessschritt 13 **ein hohes Risiko** i. S. d. Art. 35 DSGVO festgestellt wurde.

Führt die Verarbeitung personenbezogener Daten im Onlinedienst zu einem hohen Risiko, so wird eine **Datenschutz-Folgenabschätzung (DSFA)** durchgeführt. Im Einzelfall kann bereits eine „vorgefertigte“ DSFA existieren, die der Verantwortliche als eigene übernehmen oder/und an seine Bedürfnisse anpassen kann. Weitere Erleichterungen sind z. B. bei ähnlichen Verarbeitungen (Art. 35 Abs. 1 S. 2 DSGVO) oder bei einer gesetzlichen DSFA (Art. 35 Abs. 10 DSGVO) möglich. Lässt der Verantwortliche einen Teil der DSFA durch einen Auftragsverarbeiter erstellen, bleibt er dennoch auch für diesen Teil verantwortlich.

Hinsichtlich des Inhalts und der Methodik siehe **Art. 35 Abs. 7 DSGVO** sowie das **DSK Kurzpapier Nr. 5 „Datenschutz-Folgenabschätzung“.** Für die Durchführung der Datenschutz-Folgenabschätzung wird vor diesem Hintergrund folgendes Vorgehen empfohlen:

1. Festlegung des Beurteilungsumfangs (Scope) (vgl. **Standardprozessschritt 7**)
2. Bewertung der Notwendigkeit/Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck (vgl. **Standardprozessschritt 7**)
3. Identifikation der Rechtsgrundlagen (vgl. **Standardprozessschritt 8**)
4. **Modellierung der Risikoquellen** (auf Grundlage der unter **Standardprozessschritt 7** nach dem Standard-Datenschutz-Modell (SDM) modellierten Verarbeitungstätigkeiten) und unter Berücksichtigung der **Gewährleistungsziele (SDM Teil C.1)** im SDM-Würfel (SDM Teil D.2.6) (SDM Teil D.3.2.2).
5. **Risikobeurteilung** (siehe SDM Teil D.3.2.3 und DSK Kurzpapier Nr. 18)
6. **Auswahl geeigneter Abhilfemaßnahmen** (siehe z. B. die Generischen Maßnahmen nach **SDM, Teil D.1** und **SDM Bausteine; vgl. Standardprozessschritte 12 und 14**)
7. **Erstellung DSFA-Bericht** (soweit erforderlich, sollte auch bereits ein Zwischenbericht vorgelegt werden)

8. **Umsetzung der Abhilfemaßnahmen**

9. **Test und Wirksamkeitsprüfung der Abhilfemaßnahmen (inklusive Dokumentation)**

10. **Bewertung des Restrisikos und ggf. Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO**

11. **Freigabe der Verarbeitungstätigkeit**

Standardprozessschritt 16: Dokumentation in Verzeichnis von Verarbeitungstätigkeiten sowie Datenschutzkonzept mit gegebenenfalls integrierter Datenschutz-Folgenabschätzung

Punkt 5.8.1 und 5.8.2 DIN SPEC 66336 – Verzeichnis von Verarbeitungstätigkeiten und Datenschutz-Folgenabschätzung erstellen; Datenschutzkonzept entwickeln

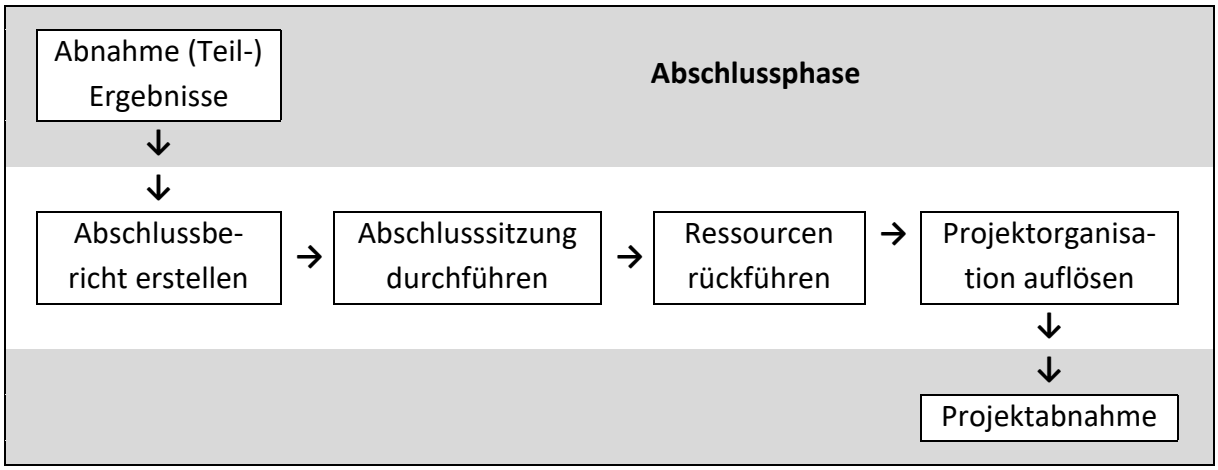
Die den Onlinedienst betreibende Behörde muss als Verantwortliche die Einhaltung der Vorgaben der DSGVO gewährleisten und dies auch nachweisen können (vgl. **Art. 5 Abs. 2 DSGVO „Rechenschaftspflicht“**). Typischerweise wird hierzu ein **Datenschutzkonzept** erstellt. In allgemeiner Hinsicht sind Verantwortliche aufgrund ihrer Rechenschaftspflicht zur Führung eines **Verzeichnisses von Verarbeitungstätigkeiten** i. S. d. **Art. 30 DGSVO** verpflichtet, auf das i. R. d. Erstellung von Datenschutzkonzepten zurückgegriffen werden kann. Sofern die i. R. d. EfA-Onlinedienstes geplante Verarbeitung personenbezogener Daten noch nicht im Verarbeitungsverzeichnis der verantwortlichen Behörde enthalten ist, muss dieses entsprechend ergänzt werden (hierzu können die Ergebnisse der **Standardprozessschritte 3 bis 9** genutzt werden.)

Hinsichtlich eines EfA-Onlinedienstes i. S. d. OZG können die **Ergebnisse der Standardprozessschritte 1 bis 15** dieses standardisierten Prüfprozesses **in einem Datenschutzkonzept dokumentiert** werden. Sofern nach **Standardprozessschritt 13** („Schwellwertanalyse“) ein hohes Risiko festgestellt und eine **Datenschutz-Folgenabschätzung (DSFA)** durchzuführen ist, kann diese direkt an das bereits erstellte Datenschutzkonzept anschließen. Dies hat den Vorteil, dass hinsichtlich einiger der für die DSFA vorgegebenen inhaltlichen Punkte auf die Dokumentation im Datenschutzkonzept verwiesen werden kann (siehe z. B. die nach Art. 35 Abs. 7 lit. a DSGVO obligatorische „systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung“).

Hinsichtlich der Struktur des Datenschutzkonzeptes mit anschließender Datenschutz-Folgenabschätzung empfiehlt **Anlage 8.1** eine **Standardstruktur**.

7 Abschlussphase

7.1 Prüfungsschritte im Rahmen der Abschlussphase



Typischerweise wird zum Ende der Durchführung oder als Teil des Projektabschlusses die Projektdokumentation archiviert (siehe z. B. Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung, S. 44).

Die **datenschutzrechtliche Dokumentation** ist hingegen nicht in dem Sinne zu archivieren, dass sie abgelegt und während des Betriebs keiner Aufmerksamkeit mehr bedarf. Vielmehr ist sie als **„lebendes Dokument“** zu verstehen und **in regelmäßig Abständen** zu **überprüfen** und, soweit erforderlich, zu ergänzen und **anzupassen**.

7.2 Zu prüfende Fragen im Rahmen der Abschlussphase

Standardprozessschritt 17: Datenschutz-Management

Insbesondere das Verzeichnis von Verarbeitungstätigkeiten und die Datenschutz-Folgenabschätzung sind auch nach Projektabschluss regelmäßig zu überprüfen und fortzuschreiben. Das ist z. B. der Fall, wenn neue Verarbeitungstätigkeiten personenbezogener Daten hinzukommen oder wegfallen, sich neue – im Laufe des Projekts nicht absehbare – Risiken ergeben oder Restrisiken durch neue TOMs weiter minimiert werden können.

Weitere Informationen zur Überprüfung und Fortschreibung der DSFA finden sich im **DSK Kurzpapier Nr. 5 „Datenschutz-Folgenabschätzung“** (S. 4).

Näheres zum **Datenschutzmanagement** bietet das **Standard-Datenschutzmodell** in **Teil D.4**.

8 Anlagen

8.1 Standardstruktur eines Datenschutzkonzeptes mit sich anschließender Datenschutz-Folgenabschätzung

1. Beschreibung des EfA-Onlinedienstes i. S. d. OZG

1.1 Liegt ein Onlinedienst i. S. d. Art. 8a Abs. 4 DSGVO vor? **(Standardprozessschritt 1)**

1.2 Wer ist die den Onlinedienst betreibende Behörde i. S. d. § 8a Abs. 4 OZG? **(Standardprozessschritt 2).**

2. Verantwortlichkeit & Auftragsverarbeitung

2.1 Welche öffentliche Stelle ist die Verantwortliche i. S. d. DSGVO? **(Standardprozessschritt 3)**

2.2 Welche Auftragsverarbeiter i. S. d. DSGVO kommen zum Einsatz? **(Standardprozessschritt 4)**

2.3 Welche Unter-Auftragsverarbeiter kommen zum Einsatz? **(Standardprozessschritt 5)**

3. Beschreibung der Verarbeitung personenbezogener Daten im Onlinedienst

3.1 Welche personenbezogenen Daten werden im Onlinedienst verarbeitet? (Kategorisierung) **(Standardprozessschritt 6)**

3.2 Wie werden die personenbezogenen Daten verarbeitet? (Modellierung der Verarbeitungstätigkeit nach SDM) **(Standardprozessschritt 7)**

4. Rechtsgrundlagen der Verarbeitung personenbezogener Daten im Onlinedienst

4.1 Dürfen die personenbezogenen Daten im Onlinedienst verarbeitet werden? (Rechtsgrundlagen des § 8a Abs. 1 OZG) **(Standardprozessschritt 8)**

4.2 Wann müssen die personenbezogenen Daten gelöscht werden? (Löschkonzept) **(Standardprozessschritt 9)**

5. Betroffenenrechte

5.1 Können die Betroffenenrechte umgesetzt werden? (Betroffenenrechtekonzept) **(Standardprozessschritt 10)**

6. Umsetzung der Prinzipien „Datenschutz durch Technikgestaltung" und „datenschutzfreundliche Voreinstellungen", Art. 25 DSGVO (Standardprozessschritt 12)

7. Risikoprüfung („Schwellwertanalyse") (Standardprozessschritt 13)

7.1 Liegt ein Fall der „Muss-Liste" der zuständigen Aufsichtsbehörde von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO vor? (siehe **Anlage 8.2.2**)

7.2 Besteht eine gesetzliche Pflicht zur Erstellung einer DSFA nach Art. 35 Abs. 3 DSGVO?

7.3 Liegt ein Fall der Liste des EDSA, Working Paper 248, rev. 01 vor?

7.4 Besteht aus sonstigen Gründen im konkreten Fall ein hohes Risiko?

7.5 Ergebnis (einfaches/ geringes Risiko → weiter mit 8. / hohes Risiko: weiter mit 8. und 9.)

8. Unabhängig vom Risiko: Welche geeigneten TOMs wurden umgesetzt? (Standardprozessschritt 14)

9. Hohes Risiko: Datenschutz-Folgenabschätzung (Standardprozessschritt 15)

9.1 Modellierung der Risikoquellen (auf Grundlage der unter Standardprozessschritt 7 nach Standard-Datenschutz-Modell (SDM) modellierten Verarbeitungstätigkeiten)

9.2 Risikobeurteilung

9.3 Auswahl geeigneter Abhilfemaßnahmen (siehe z. B. die Generischen Maßnahmen nach SDM, Teil D.1 und SDM Bausteine)

9.4 Erstellung DSFA-Bericht (soweit erforderlich, sollte auch bereits ein Zwischenbericht vorgelegt werden)

9.5 Umsetzung der Abhilfemaßnahmen

9.6 Test und Wirksamkeitsprüfung der Abhilfemaßnahmen (inklusive Dokumentation)

9.7 Bewertung des Restrisikos und ggf. Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO

9.8 Freigabe der Verarbeitungstätigkeit

10. Datenschutzmanagement (Standardprozessschritt 17)

8.2 Hilfestellungen

8.2.1 Projektmanagementhandbücher für die öffentliche Verwaltung (sofern bekannt, Stand: 10.11.2025)

- **Bund**: „Praxisleitfaden Projektmanagement für die Öffentliche Verwaltung der Bundesregierung“, abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/moderne-verwaltung/praxisleitfaden-projektmanagement.html
- **Baden-Württemberg**: „Innerdienstliche Anordnung des Innenministeriums zum Management von Projekten der Informationstechnik“ vom 21.11.2024, abrufbar unter: https://cio-bw.de/fileadmin/user_upload/medien/pdf/AnO_Projektmanagement-Leitfaden_2024.pdf
- **Bayern**: nicht bekannt
- **Berlin**: „Das Projektmanagementhandbuch des Landes Berlin - Vorgaben und Hilfestellung für Projekte der Berliner Landesverwaltung.“ – nur im internen Landesnetz abrufbar
- **Brandenburg**: „Projektmanagement-Leitfaden – Standardisierung der wesentlichen Phasen, Methoden und Begriffe für Projekte in der Brandenburger Landesverwaltung“, zu beziehen über den Brandenburgischen IT-Dienstleister
- **Bremen**: „Handbuch Projektmanagement in der Freien Hansestadt Bremen“, nicht öffentlich abrufbar
- **Hamburg**: „Projektmanagement-Handbuch der Freien und Hansestadt Hamburg“, abrufbar unter: https://epub.sub.uni-hamburg.de/epub/volltexte/2021/122930/
- **Hessen**: Projektmanagementhandbuch unter Einsatz des MIS der Hessischen Zentrale für Datenverarbeitung, abrufbar unter: https://hzd-zpm.hessen.de/vorgehensmodell
- **Mecklenburg-Vorpommern**: nicht bekannt
- **Niedersachsen**: nicht bekannt
- **Nordrhein-Westfalen**: nicht bekannt
- **Rheinland-Pfalz**: nicht bekannt
- **Saarland**: Das Projektmanagementhandbuch des Saarlands wird überarbeitet und ist zurzeit nicht öffentlich abrufbar.
- **Sachsen**: „Handbuch für Projektmanagement im Freistaat Sachsen“ – https://www.projektmanagement.sachsen.de/
- **Sachsen-Anhalt**: Das PM-Handbuch ist erstellt, aber noch nicht veröffentlicht.
- **Schleswig-Holstein**: nicht bekannt
- **Thüringen**: nicht bekannt

8.2.2 „Muss-Listen“ nach Art. 35 Abs. 4 DSGVO (Stand: 10.11.2025)

- **Bund**: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Muster/Liste_VerarbeitungsvorgaengeArt35.pdf?__blob=publicationFile&v=7
- **Baden-Württemberg**: https://www.baden-wuerttemberg.datenschutz.de/praxishilfen/#datenschutz-folgenabschaetzung
- **Bayern**: https://www.datenschutz-bayern.de/datenschutzreform2018/DSFA_Blacklist.pdf
- **Berlin**: https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/dokumente/2018-BlnBDI_DSFA-oeffentlich.pdf
- **Brandenburg**: https://www.lda.brandenburg.de/sixcms/media.php/9/DSFA-Liste_%C3%B6ffentlicher_Breich.pdf
- **Bremen**: https://www.datenschutz.bremen.de/sixcms/media.php/13/Liste%20von%20Verarbeitungsvorg%C3%A4ngen%20nach%20Artikel%2035.pdf
- **Hamburg**: https://datenschutz-hamburg.de/service-information/technisches
- **Hessen**: https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/datenschutz-folgenabschaetzung
- **Mecklenburg-Vorpommern**: https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/HilfsmittelzurUmsetzung/MV-DSFA-Muss-Liste-Oeffentlicher-Bereich.pdf
- **Niedersachsen**: https://www.lfd.niedersachsen.de/dsgvo/liste_von_verarbeitungsvorgangen_nach_art_35_abs_4_ds_gvo/muss-listen-zur-datenschutz-folgenabschatzung-179663.html
- **Nordrhein-Westfalen**: https://www.ldi.nrw.de/liste-von-verarbeitungsvorgaengen-nach-art-35-abs-4-ds-gvo-fuer-den-oeffentlichen-bereich
- **Rheinland-Pfalz**: www.datenschutz.rlp.de/themen/datenschutz-folgenabschaetzung
- **Saarland**: https://www.datenschutz.saarland.de/themen/datenschutz-folgenabschaetzung
- **Sachsen**: keine explizite Liste, Verweis auf https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf
- **Sachsen-Anhalt**: https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/Informationen/Internationales/Datenschutz-Grundverordnung/Liste_DSFA/Art-35-Liste-oeffentlicher_Bereich.pdf

- **Schleswig-Holstein**: keine explizite Liste, Verweis auf https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf
- **Thüringen**: https://tlfdi.de/fileadmin/tlfdi/datenschutz/dsfa_muss-liste_04_07_18.pdf