DSFA-Erforderlichkeitsprüfung

Prüfung der/s <Stelle> zur Erforderlichkeit der Durchführung einer Datenschutz-Folgenabschätzung (DSFA) für die Verarbeitungstätigkeit

<Verarbeitungstätigkeit>

[Dokument-ID: <ID>]

Version des Formulars: 08.03.2021

1. Beteiligte Personen und Status

1.1 An Beschreibung beteiligte Person(en) und ihre Rolle(n)	1.2 Status	1.3 Anmerkung zum Status
<Nachname>, <Vorname> [<Rolle>] <Nachname>, <Vorname> [<Rolle>]	☐ in Bearbeitung ☐ Finalisiert ☐ Sonstig: <bitte Status angeben>	

2. Anlagen bzw. Verweise zur Erforderlichkeitsprüfung

Nr.	Bezeichnung der Anlage bzw. des Verweises	Anmerkung
1		
2		
3		
4		
5		

3. Änderungshistorie

Wann?	Wer?	Was?

4. Allgemeine Angaben

4.1 Bezeichnung der Verarbeitungstätigkeit	4.2 Aktenzeichen	4.3 Auslöser der Prüfung
		☐ Neue Verarbeitung ☐ Änderung Verarbeitung ☐ Bestandsverfahren ☐ Sonstig: <sonstigen Auslöser angeben>

5. Ausnahme von der Erforderlichkeit

5.1 Sofern eine „DSFA-Whitelist“ im Sinne des Art. 35 Abs. 5 DSGVO vorhanden ist, befindet sich die betrachtete Verarbeitungstätigkeit auf dieser Liste?

☐ Ja ☐ Nein

5.2 Falls ja: Welche Fallkonstellation auf der „DSFA-Whitelist“ ist einschlägig?

⇨ V.1: Falls 5.1 bejaht wurde:
Weiterführung der Prüfung beim Punkt 9.
⇨ sonst: weiter mit Punkt 6.

6. Ausnahme von der Durchführung einer eigenen DSFA

6.1 Liegt die „Vorwegnahme“ einer DSFA im Sinn des Art. 14 BayDSG vor?

☐ Ja ☐ Nein

6.2 Falls ja: Begründung der Anwendbarkeit der einschlägigen Teilregelung des Art. 14 BayDSG

6.3 Liegt ein ähnlicher Verarbeitungsvorgang im Sinne von Art. 35 Abs. 1 S. 2 DSGVO vor?

☐ Ja ☐ Nein

6.4 Falls ja: Begründung der Anwendbarkeit des Art. 35 Abs. 1 S. 2 DSGVO

6.5 Falls 6.1 oder 6.3 bejaht wurde: Wurde die DSFA, auf die Bezug genommen wird, angepasst?

☐ Ja ☐ Nein

6.6 Falls ja: Welche Anpassungen wurden vorgenommen?

⇨ V.2: Falls 6.1 oder 6.3 bejaht wurde:
Ende der Prüfung – in Bezug genommene (Eigen-/Dritt-)DSFA muss nachgewiesen werden
⇨ sonst: weiter mit Punkt 7.

7. Erforderlichkeit ist vorgegeben

7.1 Befindet sich die betrachtete Verarbeitungstätigkeit auf der „DSFA-Blacklist“ (Art. 35 Abs. 4 DSGVO), die auch die Tatbestände des Art. 35 Abs. 3 DSGVO mit aufführt?

☐ Ja ☐ Nein

7.2 Falls ja: Welche der Fallgruppen auf der „DSFA-Blacklist“ ist einschlägig (Begründung)?

⇨ V.3 Falls 7.1 bejaht wurde:
Ende der Prüfung – eine eigene DSFA muss durchgeführt und nachgewiesen werden
⇨ sonst: weiter mit Punkt 8.

8. Eigene Risikoabschätzung durchführen (Schwellwertanalyse)

8.1 Liegt das DSFA-Kriterium „Bewerten oder Einstufen“ vor?

☐ Ja ☐ Nein

Begründung

8.2 Liegt das DSFA-Kriterium „Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung“ vor?

☐ Ja ☐ Nein

Begründung

8.3 Liegt das DSFA-Kriterium „Systematische Überwachung“ vor?

☐ Ja ☐ Nein

Begründung

8.4 Liegt das DSFA-Kriterium „Vertrauliche oder höchst persönliche Daten“ vor?

☐ Ja ☐ Nein

Begründung

8.5 Liegt das DSFA-Kriterium „Datenverarbeitung in großem Umfang“ vor?

☐ Ja ☐ Nein

Begründung

8.6 Liegt das DSFA-Kriterium „Abgleichen oder Zusammenführen von Datensätzen“ vor?

☐ Ja ☐ Nein

Begründung

8.7 Liegt das DSFA-Kriterium „Daten von schutzbedürftigen betroffenen Personen“ vor?

☐ Ja ☐ Nein

Begründung

8.8 Liegt das DSFA-Kriterium „Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen“ vor?

☐ Ja ☐ Nein

Begründung

8.9 Liegt das DSFA-Kriterium „Hinderung an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags“ vor?

☐ Ja ☐ Nein

Begründung

8.10 Liegt voraussichtlich ein hohes Risiko und damit eine DSFA-Erforderlichkeit vor?

☐ Ja ☐ Nein

Begründung

⇨ V.4 Falls 8.10 bejaht wurde:
Ende der Prüfung – eine eigene DSFA muss durchgeführt und nachgewiesen werden
⇨ sonst: weiter mit Punkt 9.

9. Durchführung einer Risikoanalyse

9.1 Wurde anstelle einer DSFA eine Risikoanalyse durchgeführt?

☐ Ja ☐ Nein

9.2 Falls ja: Verweis / Falls nein: Begründung

⇨ V.5 Falls 9. beantwortet wurde
Ende der Prüfung – eine DSFA muss nicht nachgewiesen werden

Hinweise zum Formular „DSFA-Erforderlichkeitsprüfung“

A) Allgemeines

- Nach Art. 35 Abs. 1 Satz 1 DSGVO hat der Verantwortliche bei Verarbeitungsvorgängen, die „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ haben, vorab eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen. Die Frage, ob ein Verarbeitungsvorgang die Durchführung einer DSFA erfordert, wird insbesondere bei der Einführung neuer als auch bei einer wesentlichen Änderung bestehender Verarbeitungsvorgänge relevant. Der Verantwortliche hat seine Prüfung und die Entscheidung dieser Frage nachzuweisen. Für die vereinfachte Erbringung dieses datenschutzrechtlichen Nachweises wird dieses Formular auf der **Orientierungshilfe „Datenschutz-Folgenabschätzung“ des Bayerischen Landesbeauftragten für den Datenschutz** basiert, zur Verfügung gestellt. Alle Hilfsmittel zur DSFA sind jeweils in der aktuellen Fassung auf der Homepage „https://www.datenschutz-bayern.de“ in der Rubrik „DSFA“ veröffentlicht.

- Nach der Prüfung der DSFA-Erforderlichkeit sind folgende drei unterschiedliche **Prüfergebnisse** möglich:
  a) DSFA ist nicht erforderlich (vgl. Verweis V.5)
  b) Eine bereits existierende DSFA kann – ggf. mit unwesentlichen Anpassungen –verwendet werden (vgl. Verweis V.2)
  c) Eine DSFA muss selbst vollständig durchgeführt werden (vgl. Verweise V.3 und V.4)

- Dieses Formular kann Punkt „11. Datenschutz-Folgenabschätzung“ des **Mustertextes für das Verarbeitungsverzeichnis** ergänzen, den das Bayerische Staatsministerium des Innern, für Sport und Integration (**BayStMI**) auf https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php veröffentlicht hat. Somit kann dieses Formular als Anlage zur Beschreibung einer Verarbeitungstätigkeit genutzt werden. Vor diesem Hintergrund wird im Formular grundsätzlich der **Begriff „Verarbeitungstätigkeit“** für einen Verarbeitungsvorgang im Kontext des Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO) verwendet.

- Der Begriff „**Daten**“ steht in diesem Formular für „personenbezogene Daten“.

- Der Begriff „**DSFA**“ wird in diesem Formular für „Datenschutz-Folgenabschätzung“ verwendet.

- Parameter des Einzelfalls werden in **spitzen Klammern** angegeben, z.B. „<Name>“.

B) Hinweise zu Einzelpunkten und Verweisungen

Punkt	Ausfüllhinweis
1.1	Angabe der **an der DSFA-Erforderlichkeitsprüfung beteiligten Personen** mit ihrem Namen und ihrer ausgeübten Rolle(n).
1.2	Der aktuelle **Status der Prüfung und deren Dokumentation.**
1.3	Optionale **Anmerkungen zum ausgewählten Status**.
2.	Der Unterschied zwischen einer **Anlage und einem Verweis** zur Prüfung ist, dass die Anlage fest und ausschließlich zur Prüfungsdokumentation gehört, während die verwiesenen Dokumente auch in anderen Zusammenhängen verwendet werden (Mehrfachverwendung).
3.	In der **Änderungshistorie** werden die wesentlichen Änderungen der Prüfungsdokumentation nachvollziehbar festgehalten.
4.1	Eindeutiger **Verweis auf die Beschreibung der geprüften Verarbeitungstätigkeit** im Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO).

Punkt	Ausfüllhinweis
4.2	Gegebenenfalls **Angabe des relevanten Aktenzeichens**.
4.3	Genauer **Hintergrund für diese Prüfung**.
5.1	Die für den Verantwortlichen zuständige Aufsichtsbehörde – für bayerische öffentliche Stellen also der Bayerische Landesbeauftragte für den Datenschutz – kann optional eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine DSFA erforderlich ist (Art. 35 Abs. 5 DSGVO). Ist eine solche **„DSFA-Whitelist"** vorhanden und enthält sie auch die geplante Verarbeitungstätigkeit, besteht somit keine Pflicht zur Durchführung einer DSFA. Der Bayerische Landesbeauftragte für den Datenschutz beabsichtigt derzeit nicht, eine solche Liste herauszugeben.
5.2	Angabe, welche **Fallgruppe der „DSFA-Whitelist"** zur Anwendung kommt.
6.1 – 6.2	Durch die Regelung des Art. 14 BayDSG entfällt nicht das Erfordernis einer DSFA als solches. Vielmehr wurde diese bereits im **Gesetzgebungsverfahren (Art. 14 Abs. 1 Nr. 2 BayDSG) oder durch eine andere Stelle (Art. 14 Abs. 1 Nr. 1, Abs. 2 BayDSG) durchgeführt**. Eine eigenständige DSFA durch den Verantwortlichen kann somit unterbleiben, wenn dieser eine bereits durchgeführte, geeignete DSFA „als eigene" übernimmt.
6.3 – 6.4	Eine DSFA kann auch unterbleiben, wenn eine **DSFA für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohen Risiken bereits vorhanden** ist (Art. 35 Abs. 1 Satz 2 DSGVO). Der Verantwortliche hat diese Voraussetzungen zu prüfen. Sind diese Voraussetzungen erfüllt, kann der Verantwortliche die vorhandene, bereits durchgeführte DSFA auch für die beabsichtigte Verarbeitungstätigkeit übernehmen. Das Ergebnis der Prüfung, einschließlich einer Begründung für den Verzicht auf die Durchführung einer weiteren DSFA, ist hier zu dokumentieren.
6.5 – 6.6	Auch wenn eine bereits vorliegende DSFA vom Verantwortlichen übernommen wird, ist nicht auszuschließen, dass die **schon vorliegende DSFA angepasst** werden muss. Zu beachten ist zudem, dass unter dem **Punkt „2. Anlagen bzw. Verweise zur Erforderlichkeitsprüfung" auf die in Bezug genommene (Eigen-/Dritt-)DSFA verwiesen werden muss**.
7.1	Art. 35 Abs. 4 DSGVO verpflichtet die Datenschutz-Aufsichtsbehörden, eine Liste von Verarbeitungsvorgängen zu erstellen und zu veröffentlichen, für die in jedem Fall eine Datenschutz-Folgenabschätzung erforderlich ist. Für den bayerischen öffentlichen, also insbesondere staatlichen und kommunalen Bereich veröffentlicht der Bayerische Landesbeauftragte für den Datenschutz auf Basis dieser Rechtsgrundlage die „**Bayerische Blacklist**" auf seiner Homepage https://www.datenschutz-bayern.de im Bereich „DSFA". Die ersten drei Fallgruppen dieser Liste umfassen die Tatbestände des Art. 35 Abs. 3 DSGVO.
7.2	Angabe, welche **Fallgruppe der Bayerischen Blacklist** zur Anwendung kommt.
8.1 – 8.9	Nach den **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" (**WP 248** rev.01, im Folgenden: Leitlinien), die die europäische Datenschutzgruppe nach Artikel 29 veröffentlicht und der Europäische Datenschutzausschuss gebilligt hat, müssen **neun Kriterien (DSFA-Kriterien)** berücksichtigt werden, um Verarbeitungsvorgänge zu ermitteln, für die aufgrund ihres hohen Risikos eine Datenschutz-Folgenabschätzung erforderlich ist. Näheres zu diesen neun DSFA-Kriterien, deren Anwendung sowie deren Auslegung für bayerische öffentliche Stellen findet sich in der Orientierungshilfe „Datenschutz-Folgenabschätzung", die im Bereich DSFA auf der Homepage https://www.datenschutz-bayern.de veröffentlicht ist.
8.10	Darlegung, ob nach **Bewertung und Abwägung aller vorliegenden DSFA-Kriterien**, die auf ein voraussichtlich hohes Risiko hindeuten, eine Pflicht zur DSFA besteht oder nicht besteht. Nach der Leitlinien

Punkt	Ausfüllhinweis
	ist eine DSFA in den meisten Fällen bereits obligatorisch, wenn ein Verarbeitungsvorgang zumindest zwei dieser Kriterien erfüllt. Je mehr der genannten Kriterien im Hinblick auf einen konkreten Verarbeitungsvorgang vorliegen, desto größer ist jedenfalls die Wahrscheinlichkeit, dass eine DSFA erforderlich ist. Umgekehrt kann es auch Fälle geben, in denen eine DSFA notwendig ist, obwohl nur ein Kriterium erfüllt ist oder Fälle, in denen zwar zwei oder mehr Kriterien vorliegen, gleichwohl aber nicht von einem „voraussichtlich hohen Risiko“ für die Rechte und Freiheiten natürlicher Personen und damit von der Pflicht zur Durchführung einer DSFA auszugehen ist. Für den Fall, dass unklar ist, ob eine DSFA erforderlich ist, empfehlen die Leitlinien (vgl. dort, S. 9) dennoch die Durchführung einer DSFA, weil den für die Verarbeitung Verantwortlichen damit ein hilfreiches Instrument für die Einhaltung der Datenschutzgesetze zur Verfügung steht. Näheres zu diesem Abwägungsprozess findet sich auch in der Orientierungshilfe „Datenschutz-Folgenabschätzung“, die im Bereich DSFA auf der Homepage https://www.datenschutz-bayern.de veröffentlicht ist.
9.	Nach Art. 24, Art. 25 und Art. 32 DSGVO trifft den Verantwortlichen insbesondere immer die Pflicht, geeignete technische und organisatorische Maßnahmen wirksam umzusetzen, um zum einen sicherzustellen, dass eine Verarbeitung personenbezogener Daten mit den Vorgaben der DSGVO in Einklang steht, und zum anderen ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Die Einhaltung dieser – und weiterer sich aus der DSGVO ergebender – Pflichten ist durch den Verantwortlichen angemessen in einer **Risikoanalyse** zu dokumentieren („Rechenschaftspflicht“, vgl. insbesondere Art. 5 Abs. 2, Art. 24 Abs. 1 Satz 1 DSGVO). Bei der Durchführung einer DSFA ist diese Risikoanalyse in der DSFA mit enthalten. Liegt keine DSFA-Erforderlichkeit vor, muss diese Analyse grundsätzlich eigenständig erstellt werden. Weitere Angaben hierzu finden sich in den Ausführungen „Die Datenschutz-Grundverordnung - Anforderungen an Technik und Sicherheit der Verarbeitung“, die im Bereich „Datenschutzreform 2018“ auf unserer Homepage (https://www.datenschutz-bayern.de) veröffentlicht ist.
9.1	Wurde eine datenschutzrechtliche **Risikoanalyse** für die betrachtete Verarbeitungstätigkeit **durchgeführt**?
9.2	Falls eine datenschutzrechtliche Risikoanalyse für die betrachtete Verarbeitungstätigkeit durchgeführt wurde, bitte **Fundort dieser Analyse** angeben. Falls keine solche Risikoanalyse durchgeführt wurde, bitte diesen Verzicht hier **begründen**.
V.1	Falls die betrachtete Verarbeitungstätigkeit von der relevanten „DSFA-Whitelist“ genannt wird, kann die Prüfung mit Punkt 9. Des Formulars weitergeführt werden. Wird hingegen die Verarbeitungstätigkeit nicht in einer relevanten „DSFA-Whitelist“ aufgeführt, muss die Prüfung mit Punkt 6. weitergeführt werden. Hinweis: Befindet sich die betrachtete Verarbeitungstätigkeit auf der **„DSFA-Whitelist“** im Sinne von Art. 35 Abs. 5 DSGVO, die die zuständige Datenschutzaufsichtsbehörde veröffentlicht hat, so kann die prüfende Stelle auf die Durchführung einer DSFA verzichten. In aller Regel nicht verzichtbar ist jedoch die Durchführung und der Nachweis einer datenschutzrechtlichen Risikoanalyse, die im Punkt 9. des Formulars behandelt wird.
V.2	Falls entweder 6.1 oder 6.3 bejaht werden, ist damit die **DSFA-Erforderlichkeitsprüfung beendet**. Im nächsten Schritt muss die schon vorhandene DSFA, auf die Bezug genommen werden kann, eventuell noch angepasst und in die bestehende datenschutzrechtliche Dokumentation geeignet, z.B. mittels eines entsprechenden Verweises oder Anpassungsdokuments, integriert und die einschlägigen Schutzmaßnahmen wirksam umgesetzt werden. Ist keine DSFA vorhanden, auf die Bezug genommen werden kann, d.h. 6.1 und 6.3 werden verneint, muss die Prüfung mit dem Punkt 7. Des Formulars fortgeführt werden.

Punkt	Ausfüllhinweis
V.3	Befindet sich die betrachtete Verarbeitungstätigkeit auf der „DSFA-Blacklist“ (Art. 35 Abs. 4 DSGVO), welche die zuständige Datenschutzaufsichtsbehörde veröffentlicht hat, ist die Erforderlichkeitsprüfung zu Ende und es muss eine **eigene DSFA durchgeführt** und nachgewiesen werden. Fällt die betrachtete Verarbeitungstätigkeit unter keine Fallgruppe der relevanten „DSFA-Blacklist“, so ist die Prüfung mit dem Punkt 8. des Formulars fortzuführen.
V.4	Falls die Schwellwertanalyse zum Ergebnis geführt hat, dass die betrachtete Verarbeitungstätigkeit voraussichtlich ein hohes Risiko zur Folge hat, ist die Erforderlichkeitsprüfung zu Ende und es muss eine **eigene DSFA durchgeführt** und nachgewiesen werden. Falls die Schwellwertanalyse zum Ergebnis geführt hat, dass die betrachtete Verarbeitungstätigkeit voraussichtlich kein hohes Risiko zur Folge hat, ist die Prüfung mit dem Punkt 9. des Formulars fortzuführen.
V.5	Auch der Prüfungsstrang, der zu keiner DSFA-Erforderlichkeit geführt hat, ist nun beendet.