Der Bayerische Landesbeauftragte
für den Datenschutz

Datenschutz-Folgenabschätzung

Orientierungshilfe

Stand: 25. Mai 2018

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

Einleitung

Mit einer Datenschutz-Folgenabschätzung (DSFA) wird die Verarbeitung von personenbezogenen Daten in einem folgenabschätzungspflichtigen Verarbeitungsvorgang beschrieben und bewertet. Dabei müssen insbesondere die Risiken für die Rechte und Freiheiten natürlicher Personen, die durch den Verarbeitungsvorgang auftreten, bewertet und durch geeignete Gegenmaßnahmen ausreichend eingedämmt werden.

Der Verantwortliche für den jeweiligen Verarbeitungsvorgang kann damit nachweisen, dass er geeignete Maßnahmen ausgewählt hat, so dass eine regelungskonforme Verarbeitung möglich ist.

Eine DSFA bezieht sich auf die verarbeiteten Daten, die verwendete Hard- und Software und die eingesetzten Prozesse eines konkreten Verarbeitungsvorgangs. Für mehrere ähnliche Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige DSFA durchgeführt werden („kumulierte DSFA“, siehe Art. 35 Abs. 1 Satz 2 Datenschutz-Grundverordnung – DSGVO).

Die Datenschutz-Folgenabschätzung

1. Erforderlichkeit einer Datenschutz-Folgenabschätzung (einschließlich Prüfschema)

Die Erforderlichkeit zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) ist nicht mit derjenigen einer datenschutzrechtlichen Freigabe nach dem bisherigen Art. 26 Bayerisches Datenschutzgesetz (BayDSG) gleichzusetzen. Im Unterschied zum bisherigen Datenschutzrecht betont die Datenschutz-Grundverordnung (DSGVO) den risikobasierten Ansatz bei der Bewertung der datenschutzgerechten Durchführung einer Datenverarbeitung. Die Durchführung einer DSFA ist grundsätzlich zwingend (nur) bei (vermuteten) „Hochrisikoverarbeitungen“:

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 DSFA durchzuführen. Das hohe Risiko kann hierbei aus der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung resultieren, insbesondere wenn neue Technologien verwendet werden.

Die Frage, ob ein Verarbeitungsvorgang die Durchführung einer DSFA erfordert, wird sowohl bei der Einführung neuer als auch bei einer wesentlichen Änderung bestehender Verarbeitungsvorgänge relevant. Für die Prüfung und Entscheidung dieser Frage bietet sich die nachfolgend aufgezeigte Prüfreihenfolge an.

Das Ergebnis dieser „Vorprüfung“ (nicht zu verwechseln mit der eigentlichen Durchführung einer DSFA!) ist insbesondere auch dann zu dokumentieren, wenn der Verantwortliche zu der Auffassung gelangt, dass ein Verarbeitungsvorgang nicht folgenabschätzungspflichtig ist. Zur Erfüllung dieses Dokumentationserfordernisses kann auf das vom Bayerischen Staatsministerium des Innern und für Integration herausgegebene Musterformular für die Beschreibung einer Verarbeitungstätigkeit zurückgegriffen werden (im Internet abrufbar von der Homepage des Bayerischen Landesbeauftragten für den Datenschutz unter „Datenschutzreform 2018“). Dieses Formular sieht unter Nr. 11 eine entsprechende Eintragung vor.

Zuvor muss der Verantwortliche natürlich prüfen, auf welche Rechtsgrundlage er die beabsichtigte Datenverarbeitung stützt. Kommt keine Rechtsgrundlage in Betracht, hat die Verarbeitung ohnehin zu unterbleiben.

a) Datenschutz-Folgenabschätzung nicht erforderlich

Zunächst bietet es sich an zu prüfen, ob die Pflicht zur Durchführung einer DSFA für den beabsichtigten Verarbeitungsvorgang anhand eines der nachfolgenden Kriterien ausgeschlossen werden kann.

Die Datenschutz-Folgenabschätzung

Art. 14 BayDSG-neu

Nach Art. 14 des neugefassten Bayerischen Datenschutzgesetzes (BayDSG-neu) kann die Durchführung einer eigenen DSFA durch den Verantwortlichen unterbleiben, soweit

- eine solche für den Verarbeitungsvorgang bereits vom fachlich zuständigen Staatsministerium oder einer von diesem ermächtigten öffentlichen Stelle durchgeführt wurde und dieser Verarbeitungsvorgang im Wesentlichen unverändert übernommen wird (Art. 14 Abs. 1 Nr. 1 BayDSG-neu),
- ein automatisiertes Verfahren, das zum Einsatz durch öffentliche Stellen bestimmt ist, durch eine öffentliche Stelle (z. B. die Anstalt für Kommunale Datenverarbeitung in Bayern - AKDB) entwickelt wurde, die entwickelnde Stelle eine DSFA durchgeführt hat und das Verfahren im Wesentlichen unverändert übernommen wird (Art. 14 Abs. 2 BayDSG-neu),
- der konkrete Verarbeitungsvorgang in einer Rechtsvorschrift geregelt ist und im Rechtsetzungsverfahren bereits eine DSFA erfolgt ist, es sei denn, dass in der Rechtsvorschrift etwas anderes bestimmt ist (Art. 14 Abs. 1 Nr. 2 BayDSG-neu).

Durch die Regelung des Art. 14 BayDSG-neu entfällt also nicht das Erfordernis einer DSFA als solches. Vielmehr wurde diese bereits im Gesetzgebungsverfahren (Art. 14 Abs. 1 Nr. 2 BayDSG-neu) oder durch eine andere Stelle (Art. 14 Abs. 1 Nr. 1, Abs. 2 BayDSG-neu) durchgeführt. Eine weitere DSFA durch den Verantwortlichen kann somit unterbleiben, wenn dieser eine bereits durchgeführte DSFA „als eigene“ übernimmt.

Hierfür müssen dem Verantwortlichen die Ergebnisse der bereits vorgenommenen DSFA in geeigneter Weise zur Verfügung gestellt werden. Der Verantwortliche hat dann zu prüfen, ob die ihm zur Verfügung gestellten Unterlagen hinsichtlich des von ihm beabsichtigten Verarbeitungsvorgangs den Anforderungen des Art. 35 DSGVO genügen. Ist dies der Fall und verzichtet er daraufhin auf eine eigene DSFA, hat der Verantwortliche das Ergebnis der vorgenannten Überprüfung zu dokumentieren (vgl. Gesetzesbegründung zu Art. 14 BayDSG-neu, Landtags-Drucksache 17/19628, S. 38).

Im Fall einer „gesetzlich“ durchgeführten DSFA (Art. 14 Abs. 1 Nr. 2 BayDSG-neu, vgl. auch Art. 35 Abs. 10 DSGVO) hat der Verantwortliche zumindest zu dokumentieren, dass der konkrete Verarbeitungsvorgang tatsächlich in einer Rechtsvorschrift geregelt ist, für die im Zuge des Rechtsetzungsverfahren eine DSFA erfolgt ist.

„Whitelist“

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; zu dieser sogenannten „Whitelist“ siehe auch unten). Ist eine solche „Whitelist“ vorhanden und enthält sie auch den beabsichtigten Verarbeitungsvorgang, besteht somit keine Pflicht zur Durchführung einer DSFA.

DSFA für ähnlichen Verarbeitungsvorgang bereits vorhanden

Eine weitere 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. Diese Prüfung umfasst notwendigerweise auch eine Risikobeurteilung des beabsichtigten Verarbeitungsvorgangs, damit der Verantwortliche beurteilen kann, ob der ähnliche Verarbeitungsvorgang tatsächlich „ähnlich hohe Risiken" aufweist. Ist dies der Fall, kann der Verantwortliche die vorhandene, bereits durchgeführte DSFA auch für den beabsichtigten Verarbeitungsvorgang übernehmen. Das Ergebnis der Prüfung, einschließlich einer Begründung für den Verzicht auf die Durchführung einer weiteren DSFA, ist zu dokumentieren.

b) Datenschutz-Folgenabschätzung erforderlich

Liegt keiner der dargestellten „Ausschlusstatbestände" vor, ist in einem nächsten Schritt „positiv" zu prüfen, ob eine Pflicht zur Durchführung einer DSFA besteht. Dies ist der Fall, wenn ein Verarbeitungsvorgang „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge" hat.

Art. 35 Abs. 3 DSGVO

Bei bestimmten Verarbeitungsvorgängen geht der europäische Gesetzgeber davon aus, dass diese stets mit einem voraussichtlich hohen Risiko verbunden sind. Nach Art. 35 Abs. 3 DSGVO ist eine DSFA in den folgenden Fällen zwingend erforderlich:

- bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen (Art. 35 Abs. 3 Buchst. a DSGVO);
- bei einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO (Art. 35 Abs. 3 Buchst. b DSGVO);
- bei einer systematischen umfangreichen Überwachung öffentlich zugänglicher Bereiche (Art. 35 Abs. 3 Buchst. c DSGVO).

Lässt sich ein Verarbeitungsvorgang einer der in Art. 35 Abs. 3 DSGVO genannten Fallgruppen zuordnen, hat der Verantwortliche in jedem Fall eine DSFA durchzuführen. Einer eigenen „Vorab-Prüfung" durch den Verantwortlichen, ob der Verarbeitungsvorgang „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen" zur Folge hat, bedarf es in diesen Fällen nicht.

Die Datenschutz-Folgenabschätzung

Anmerkung: Unabhängig hiervon hat der Verantwortliche für jede von ihm verantwortete Verarbeitung personenbezogener Daten die mit dieser einhergehenden Risiken für die Rechte und Freiheiten natürlicher Personen zu beurteilen, etwa um geeignete technische und organisatorische Maßnahmen nach Art. 24 und 32 DSGVO treffen zu können. Vgl. ausführlich hierzu bereits den Informationsbeitrag „Die Datenschutz-Grundverordnung (DSGVO) – Anforderungen an Technik und Sicherheit der Verarbeitung", der von der Homepage des Bayerischen Landesbeauftragten für den Datenschutz unter „Datenschutzreform 2018" abrufbar ist.

„Blacklist"

Der Bayerische Landesbeauftragte für den Datenschutz erstellt als Aufsichtsbehörde über die bayerischen öffentlichen Stellen eine Liste mit Verarbeitungsvorgängen, bei denen stets eine DSFA durchzuführen ist („Blacklist", Art. 35 Abs. 4 DSGVO). Diese Liste wird auf der Homepage des Landesbeauftragten veröffentlicht. Die „Blacklist" ist nicht abschließend und wird im erforderlichen Umfang fortlaufend aktualisiert.

Befindet sich der beabsichtigte Verarbeitungsvorgang auf dieser „Blacklist", ist der Verantwortliche zur Durchführung einer DSFA verpflichtet. Die Beurteilung, ob der Verarbeitungsvorgang „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen" zur Folge hat, ist in diesen Fällen bereits durch die Aufsichtsbehörde erfolgt und wird dem Verantwortlichen insoweit abgenommen.

Eigene Risikoabschätzung

Weder Art. 35 Abs. 3 DSGVO noch die „Blacklist" sind abschließend. Unterfällt ein Verarbeitungsvorgang somit weder Art. 35 Abs. 3 DSGVO noch der „Blacklist", hat der Verantwortliche eigenständig abzuschätzen, ob die geplante Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt und somit die Pflicht zur Durchführung einer DSFA besteht. Hierbei sind die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung zu berücksichtigen (siehe Art. 35 Abs. 1 Satz 1 DSGVO). Die Risiken sind sowohl hinsichtlich ihrer jeweiligen Schwere als auch ihrer jeweiligen Eintrittswahrscheinlichkeit zu beurteilen (vgl. Erwägungsgrund 90 DSGVO). Ausreichend, aber auch erforderlich ist in diesem Zusammenhang eine Risikoabschätzung im Sinne einer „Schwellwertanalyse".

Hierfür können die „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" (im Folgenden: Working Paper 248 Rev. 01, im Internet abrufbar von der Homepage des Bayerischen Landesbeauftragten für den Datenschutz unter „Datenschutzreform 2018") der europäischen „Datenschutzgruppe nach Artikel 29" als Auslegungshilfe herangezogen werden. Bei der Beurteilung der Frage, ob ein Verarbeitungsvorgang voraussichtlich ein hohes Risiko mit sich bringt, sind demnach die folgenden neun Kriterien zu berücksichtigen (siehe ausführlich Working Paper 248 Rev. 01, S. 9 ff.):

(1) Bewerten und Einstufen

Hierunter fällt auch das Erstellen von Profilen und Prognosen, insbesondere auf der Grundlage von „Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person“ (vgl. Erwägungsgründe 71 und 91 DSGVO).

Beispiel: Eine Behörde erstellt anhand der Nutzung ihrer Website personenbezogene Verhaltensprofile.

(2) Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung

Dies umfasst Verarbeitungen, auf deren Grundlage für Betroffene Entscheidungen getroffen werden sollen, „die Rechtswirkung gegenüber natürlichen Personen entfalten“ oder diese „in ähnlich erheblicher Weise beeinträchtigen“ (vgl. Art. 35 Abs. 3 Buchst. a DSGVO). So kann die Verarbeitung beispielsweise zum Ausschluss oder zur Benachteiligung von Personen führen. Verarbeitungsvorgänge, die keine oder wenige Auswirkungen auf Personen haben, erfüllen nicht dieses spezielle Kriterium.

(3) Systematische Überwachung

Dies betrifft Verarbeitungsvorgänge, die die Beobachtung, Überwachung oder Kontrolle von betroffenen Personen zum Ziel haben und auf beispielsweise über Netzwerke erfasste Daten oder auf „eine systematische […] Überwachung öffentlich zugänglicher Bereiche“ (vgl. Art. 35 Abs. 3 Buchst. c DSGVO) zurückgreifen.

(4) Vertrauliche oder höchst persönliche Daten

Hierzu zählen besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DSGVO (z. B. Informationen über die politischen Meinungen von Einzelpersonen) sowie personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten im Sinne von Art. 10 DSGVO.

Beispiel: Ein Krankenhaus archiviert die Krankenakten seiner Patienten.

Auch weitere Datenkategorien, die zwar nicht in den Art. 9 und 10 DSGVO aufgeführt sind, jedoch die möglichen Risiken für die Rechte und Freiheiten natürlicher Personen erhöhen können, sind – je nach Fallgestaltung – diesem Kriterium zuzuordnen. Dies kann etwa auch Standort- oder Finanzdaten betreffen. Zu berücksichtigen ist in diesem Zusammenhang unter anderem, ob Daten durch die betroffene Person bereits öffentlich zugänglich gemacht worden sind.

(5) Datenverarbeitung in großem Umfang

Bei Beurteilung der Frage, ob eine Datenverarbeitung „in großem Umfang“ erfolgt, sind insbesondere die folgenden Faktoren zu berücksichtigen:

(a) Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil an der entsprechenden Bevölkerungsgruppe;
(b) verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente;
(c) Dauer oder Dauerhaftigkeit der Datenverarbeitung;
(d) geografisches Ausmaß der Datenverarbeitung.

(6) Abgleichen oder Zusammenführen von Datensätzen

Dies betrifft beispielsweise Datensätze, die aus zwei oder mehreren Datenverarbeitungsvorgängen stammen, die zu unterschiedlichen Zwecken und/oder von verschiedenen für die Datenverarbeitung Verantwortlichen durchgeführt wurden, und zwar in einer Weise, die über die vernünftigen Erwartungen der Betroffenen hinausgeht.

(7) Daten von schutzbedürftigen betroffenen Personen (vgl. Erwägungsgrund 75 DSGVO)

Als schutzbedürftige betroffene Personen gelten beispielsweise folgende Bevölkerungsgruppen: Kinder und Personen mit besonderem Schutzbedarf (psychisch Kranke, Asylbewerber, Senioren, Patienten usw.).

(8) Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen

Hierunter fällt beispielsweise die Kombination aus Fingerabdruck- und Gesichtserkennung zum Zwecke einer verbesserten Zugangskontrolle. Aus Art. 35 Abs. 1 DSGVO und Erwägungsgründen 89 und 91 DSGVO wird deutlich, dass der Einsatz einer neuen Technologie, die „entsprechend dem jeweils aktuellen Stand der Technik“ (Erwägungsgrund 91 DSGVO) als solche einzuordnen ist, der Grund für die Notwendigkeit einer DSFA sein kann.

(9) Betroffene Personen werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert

(Vgl. Art. 22 DSGVO und Erwägungsgrund 91 DSGVO). Hierzu zählen beispielsweise Verarbeitungsvorgänge, mit deren Hilfe betroffenen Personen der Zugriff auf eine Dienstleistung gestattet oder verwehrt werden soll.

Nach Auffassung der „Datenschutzgruppe nach Artikel 29“ 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 na-

türlicher Personen und damit von der Pflicht zur Durchführung einer DSFA auszugehen ist. Die dargestellten Kriterien sind somit eine Hilfestellung für den Verantwortlichen, um einzuschätzen, ob ein Verarbeitungsvorgang „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat.

Trifft ein Verantwortlicher auf der Grundlage seiner Risikoabschätzung die Entscheidung, keine DSFA durchzuführen, muss er dies begründen und die Entscheidung insbesondere mit der der Entscheidung zugrundeliegenden Risikoanalyse dokumentieren. Dabei ist auch die Stellungnahme des behördlichen Datenschutzbeauftragten beizufügen.

c) Zusammenfassung: Prüfschema

Zur Beurteilung der Frage, ob ein Verarbeitungsvorgang die Durchführung einer DSFA erfordert, bietet sich zusammenfassend die nachfolgende Prüfreihenfolge an:

(1) Unterfällt der Verarbeitungsvorgang einem Tatbestand des Art. 14 BayDSG-neu?

Ja: keine weitere DSFA erforderlich, vorhandene DSFA „als eigene“ übernehmen.
Nein: Prüfung fortsetzen.

(2) Liegt eine „Whitelist“ des Bayerischen Landesbeauftragten für den Datenschutz (Art. 35 Abs. 5 DSGVO) vor und wird der Verarbeitungsvorgang von ihr erfasst?

Ja: Vorgang bedarf keiner DSFA.
Nein: Prüfung fortsetzen.

(3) Ist für einen ähnlichen Verarbeitungsvorgang mit ähnlich hohen Risiken bereits eine DSFA vorhanden?

Ja: Die vorhandene DSFA kann auch für den beabsichtigten Verarbeitungsvorgang übernommen werden.
Nein: Prüfung fortsetzen.

(4) Unterfällt der Verarbeitungsvorgang einem Tatbestand des Art. 35 Abs. 3 DSGVO?

Ja: DSFA ist durchzuführen.
Nein: Prüfung fortsetzen.

(5) Wird der Verarbeitungsvorgang von der „Blacklist“ des Bayerischen Landesbeauftragten für den Datenschutz (Art. 35 Abs. 4 DSGVO) erfasst?

Ja: DSFA ist durchzuführen.
Nein: Prüfung fortsetzen.

(6) Hat der Verarbeitungsvorgang auf Grundlage einer eigenen Risikoabschätzung des Verantwortlichen „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen“ zur Folge?

Ja: DSFA ist durchzuführen.
Nein: Keine DSFA erforderlich, Prüfung beendet.

Das Ergebnis des Prüfprozesses sowie in erforderlichem Umfang dessen Begründung ist hinreichend zu dokumentieren (vgl. oben).

2. Die Datenschutz-Folgenabschätzung als kontinuierlicher Prozess

Ändern sich die Risiken im Hinblick auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung, so ist es bei Vorliegen der gesetzlichen Voraussetzungen grundsätzlich erforderlich, eine DSFA auch bei bereits laufenden Verfahren erneut durchzuführen. Die Durchführung einer DSFA ist keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess.

3. Verarbeitungsvorgänge, die bereits vor dem 25. Mai 2018 durchgeführt wurden („Bestandsverfahren“)

Für bereits laufende, nach Art. 26 BayDSG freigegebene Verarbeitungsvorgänge, die ohne wesentliche Änderungen fortgeführt werden und die künftig eine DSFA erfordern, ist diese in einer Übergangsfrist spätestens bis zum 25. Mai 2021 nachzuholen.

4. Durchführung einer Datenschutz-Folgenabschätzung

Die DSFA ist „vorab“, also vor dem Einsatz bzw. der wesentlichen Änderung einer Verarbeitung durchzuführen.

a) Beteiligte Personen

Für die Erstellung einer DSFA benötigt man Kenntnisse sowohl im Datenschutzrecht als auch in den Fachprozessen des Verfahrens. Idealerweise wirken mehrere Personen bei der Entwicklung der DSFA mit, gegebenenfalls auch externe Dienstleister. Der behördliche Datenschutzbeauftragte berät den Verantwortlichen im Zusammenhang mit der DSFA und überwacht deren Durchführung (Art. 35 Abs. 2, Art. 39 Abs. 1 Buchst. c DSGVO). Die eigentliche Durchführung der DSFA obliegt aber dem Verantwortlichen.

Soweit angebracht, müssen auch die betroffenen Personen oder ihre Vertreter (dies umfasst auch Interessenvertreter) befragt werden; zumindest muss deren Blickwinkel auf das Verfahren berücksichtigt werden (Art. 35 Abs. 9 DSGVO).

b) Inhalt

Eine DSFA muss mindestens enthalten (Art. 35 Abs. 7 DSGVO):

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35 Abs. 1 DSGVO und
- 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 diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Eine DSFA betrachtet die Risiken aus der Sicht der betroffenen Personen, wohingegen bei der Informationssicherheit primär der Schwerpunkt auf die Risiken für die Organisation gelegt wird.

c) Methoden

Der Verantwortliche kann die Methode zur Erstellung einer DSFA frei wählen, muss aber sicherstellen, dass alle gesetzlichen Mindestanforderungen erfüllt werden. Insbesondere muss die Vollständigkeit der Modellierung sichergestellt werden, also Maßnahmen, Risiken und Bedrohungen dargestellt werden. Deshalb ist eine strukturierte Methode unerlässlich. Mit Hilfe der Anlage 2 „Kriterien für eine zulässige Datenschutz-Folgenabschätzung“ des Working Paper 248 Rev. 01 können Methoden geprüft werden.

Beispiele für EU-weite allgemeine Methoden sind danach unter anderem:

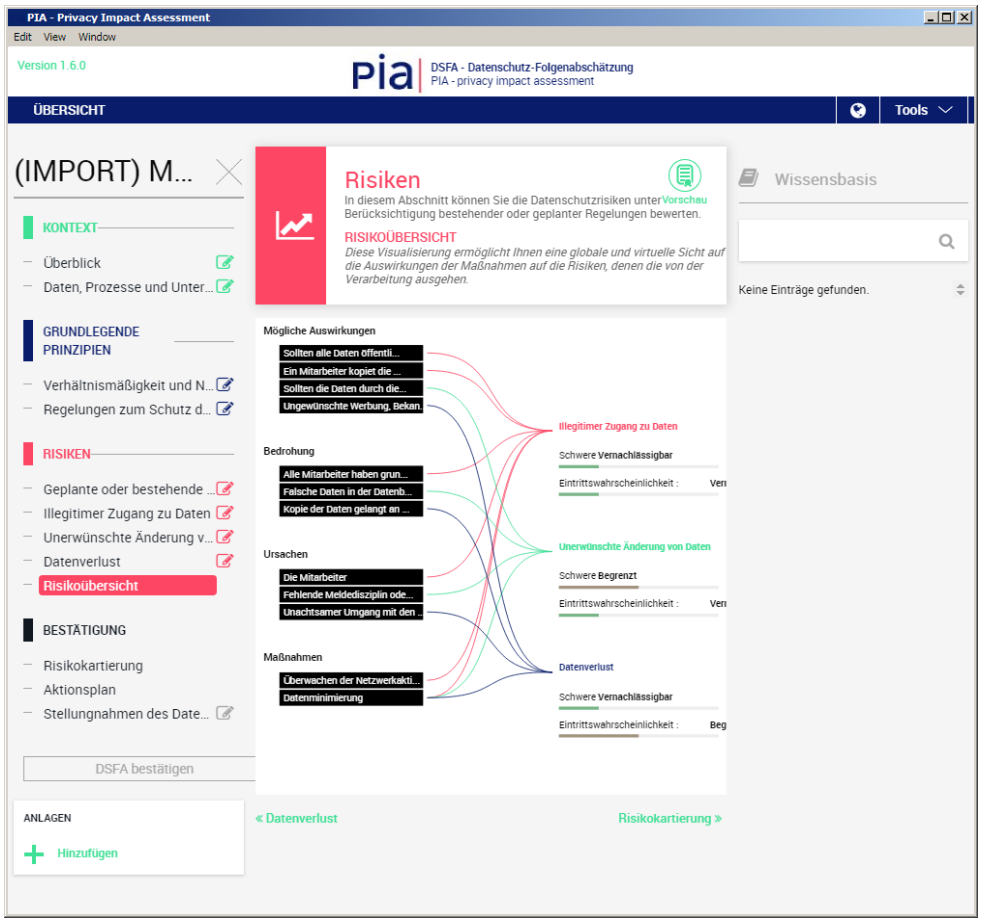
- das „Standard-Datenschutzmodell (SDM)“ der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder,
- der „Conducting privacy impact assessments code of practice“ der Datenschutzaufsichtsbehörde des Vereinigten Königreichs,
- die „Privacy Impact Assessment (PIA)” der französischen Datenschutzaufsichtsbehörde Commission nationale de l’informatique et des libertés (CNIL).

Die Methodik der CNIL bietet neben einer umfangreichen Dokumentation auch eine Software-Unterstützung, so dass der komplette Zyklus der Erstellung einer DSFA in Software durchgeführt und dokumentiert werden kann. Die Software („PIA-Tool“) ermöglicht es, eine vollständige DSFA (im Englischen: Privacy Impact Assessment – PIA) durchzuführen, und stellt sicher, dass alle nötigen Kriterien für eine DSFA enthalten sind.

Die Datenschutz-Folgenabschätzung

Die Software kann frei verwendet und weiterentwickelt werden (GPL v3.0) und ist für Windows, Linux und für Mac OS als eigenständiges Programm sowie auch als Web-Anwendung verfügbar. Sie kann auf der Homepage des Bayerischen Landesbeauftragten für den Datenschutz unter „Datenschutzreform 2018“ in einer von der Aufsichtsbehörde geprüften deutschen Version heruntergeladen werden. Auf der Webseite der CNIL finden sich darüber hinaus Informationen zum PIA-Tool und zur Durchführung einer DSFA in französischer und englischer Sprache (https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment bzw. https://www.cnil.fr/en/PIA-privacy-impact-assessment-en).

Sowohl die Software als auch die Übersetzung ist aktuell noch in Entwicklung („beta“), kann aber auch jetzt schon als Hilfe für die Erstellung einer DSFA genutzt werden.



d) Beteiligung des Bayerischen Landesbeauftragten für den Datenschutz

Nur in Fällen, in denen der Verantwortliche keine hinreichenden Maßnahmen trifft, um ein sich aus einer DSFA hervorgehendes hohes Risiko einzudämmen, ist eine Konsultation des Bayerischen Landesbeauftragten für den Datenschutz erforderlich (Art. 36 Abs. 1 DSGVO). Insbesondere hier kann es hilfreich sein, die durchgeführte DSFA mit dem oben genannten PIA-Tool zu modellieren und das Ergebnis an den Landesbeauftragten zu senden.

Anhang: Vorschriften

Artikel 35 DSGVO
Datenschutz-Folgenabschätzung

(1) Hat eine 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, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder
c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
d) 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 diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Artikel 36 DSGVO
Vorherige Konsultation

(1) Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung gemäß Artikel 35 hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.

(2) Falls die Aufsichtsbehörde der Auffassung ist, dass die geplante Verarbeitung gemäß Absatz 1 nicht im Einklang mit dieser Verordnung stünde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder nicht ausreichend eingedämmt hat, unterbreitet sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von bis zu acht Wochen nach Erhalt des Ersuchens um Konsultation entsprechende schriftliche Empfehlungen und kann ihre in Artikel 58 genannten Befugnisse ausüben. Diese Frist kann unter Berücksichtigung der Komplexität der geplanten Verarbeitung

um sechs Wochen verlängert werden. Die Aufsichtsbehörde unterrichtet den Verantwortlichen oder gegebenenfalls den Auftragsverarbeiter über eine solche Fristverlängerung innerhalb eines Monats nach Eingang des Antrags auf Konsultation zusammen mit den Gründen für die Verzögerung. Diese Fristen können ausgesetzt werden, bis die Aufsichtsbehörde die für die Zwecke der Konsultation angeforderten Informationen erhalten hat.

(3) Der Verantwortliche stellt der Aufsichtsbehörde bei einer Konsultation gemäß Absatz 1 folgende Informationen zur Verfügung:

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.

(4) Die Mitgliedstaaten konsultieren die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für von einem nationalen Parlament zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regelungsmaßnahmen, die die Verarbeitung betreffen.

(5) Ungeachtet des Absatzes 1 können Verantwortliche durch das Recht der Mitgliedstaaten verpflichtet werden, bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit, die Aufsichtsbehörde zu konsultieren und deren vorherige Genehmigung einzuholen.

Erwägungsgründe 89 bis 91 DSGVO

(89) Gemäß der Richtlinie 95/46/EG waren Verarbeitungen personenbezogener Daten bei den Aufsichtsbehörden generell meldepflichtig. Diese Meldepflicht ist mit einem bürokratischen und finanziellen Aufwand verbunden und hat dennoch nicht in allen Fällen zu einem besseren Schutz personenbezogener Daten geführt. Diese unterschiedslosen allgemeinen Meldepflichten sollten daher abgeschafft und durch wirksame Verfahren und Mechanismen ersetzt werden, die sich stattdessen vorrangig mit denjenigen Arten von Verarbeitungsvorgängen befassen, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Zu solchen Arten von Verarbeitungsvorgängen gehören insbesondere solche, bei denen neue Technologien eingesetzt werden oder die neuartig sind und bei denen der Verantwortliche noch keine Datenschutz-Folgenabschätzung durchgeführt hat bzw. bei denen aufgrund der seit der ursprünglichen Verarbeitung vergangenen Zeit eine Datenschutz-Folgenabschätzung notwendig geworden ist.

(90) In derartigen Fällen sollte der Verantwortliche vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen, mit der die spezifische Eintrittswahrscheinlichkeit und die

Schwere dieses hohen Risikos unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos bewertet werden. Diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll.

(91) Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und — beispielsweise aufgrund ihrer Sensibilität — wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln verarbeitet werden. Gleichermaßen erforderlich ist eine Datenschutz-Folgenabschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.

Art. 14 BayDSG-neu
Datenschutz-Folgenabschätzung
(zu Art. 35 DSGVO)

(1) Eine Datenschutz-Folgenabschätzung (Folgenabschätzung) durch den Verantwortlichen kann unterbleiben, soweit

1. eine solche für den Verarbeitungsvorgang bereits vom fachlich zuständigen Staatsministerium oder einer von diesem ermächtigten öffentlichen Stelle durchgeführt wurde und dieser Verarbeitungsvorgang im Wesentlichen unverändert übernommen wird oder

2. der konkrete Verarbeitungsvorgang in einer Rechtsvorschrift geregelt ist und im Rechtsetzungsverfahren bereits eine Folgenabschätzung erfolgt ist, es sei denn, dass in der Rechtsvorschrift etwas anderes bestimmt ist.

(2) [1]Entwickelt eine öffentliche Stelle ein automatisiertes Verfahren, das zum Einsatz durch öffentliche Stellen bestimmt ist, so kann sie, sofern die Voraussetzungen des Art. 35 Abs. 1 DSGVO bei diesem Verfahren vorliegen, die Folgenabschätzung nach den Art. 35 und 36 DSGVO durchführen. [2]Soweit das Verfahren von öffentlichen Stellen im Wesentlichen unverändert übernommen wird, kann eine weitere Folgenabschätzung durch die übernehmenden öffentlichen Stellen unterbleiben.