 

  DFN-CERT Services GmbH Logo

DSFA − Datenschutz-Folgeabschätzung

Grundlagen, Methodik

Version 1.0, 09. November 2018

Die Nutzung dieses Dokuments ist zulässig unter der Lizenz CC BY-SA 3.0    
<https://creativecommons.org/licenses/by-sa/3.0/de/legalcode>   
Autor: NRW Projektgruppe „Umsetzung der EU-Datenschutz-Grundverordnung (EU-DSGVO) −  
Datenschutzmanagementsysteme“ 2018

gefördert vom 

DSFA − Datenschutz-Folgeabschätzung

# Rechtliche Grundlagen

Art. 35 DSGVO verlangt eine DSFA, wenn die Form der Verarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen hat, insbesondere:

* Verwendung neuer Technologien
* Art,
* Umfang,
* Umstände,
* Zwecke

Diese Merkmale sind so abstrakt, dass ohne weitere Konkretisierung keine praktische Anwendbarkeit gegeben ist. Eine durch die Datenschutzaufsichtsbehörden anerkannte Konkretisierung erfolgt durch die „Leitlinien zur Datenschutz-Folgeabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 wahrscheinlich ein hohes Risiko mit sich bringt“ der Art. 29 Datenschutzgruppe vorgenommen. Allerdings sind die 9 dort genannten Fallgruppen eines potenziell hohen Risikos ebenfalls teilweise sehr abstrakt bestimmt. Einigermaßen konkret sind nur die Fälle, in denen nach Art. 35 Abs. 3 und 4 DSGVO stets eine DSFA durchgeführt werden muss. Abseits dieser Fälle, muss anhand der Kriterien in Art. 35 Abs. 1 DSGVO und den hierzu verfügbaren Konkretisierungen eine sog. Schwellwertanalyse durchgeführt werden um zu ermitteln, ob eine DSFA für die zu prüfende Verarbeitung durchzuführen ist.

# Schwellwertanalyse

Die Schwellwertanalyse ergibt sich nicht direkt aus dem Gesetz, ist aber logische Folge aus Art. 35 Abs. 1 DSGVO. Die Schwellwertanalyse ist systematisch vergleichbar mit der Schutzbedarfsanalyse aus der Informationssicherheit, verfolgt aber einen anderen Fokus, indem das Risiko von Grundrechtsverletzungen des Betroffenen im Mittelpunk steht.

|  |  |
| --- | --- |
| Schwellwertanalyse | Schutzbedarfsanalyse |
| Fokus: Risiko für Rechte und Freiheiten von betroffenen natürlichen Personen | Fokus: Risiken für die Organisation |
| Schwellwert über- oder unterschritten:  Bei Unterschreitung: Normaler Schutzbedarf, Prüfung endet hier, im Datenschutz gibt es keinen Schutzbedarf unterhalb normal, weil stets personenbezogene Daten betroffen sind  Bei Überschreitung: Hoher bzw. sehr hoher Schutzbedarf, DSFA erforderlich | Schutzbedarf:  Niedrig  Normal  Hoch: Risikoanalyse erforderlich  Sehr hoch: Risikoanalyse erforderlich |
| Kriterien: Art. 35 Abs. 1, 3 und 4 DSGVO | Kriterien: Informationssicherheit (Eintrittswahrscheinlichkeit/Schadenshöhe) |

# Bei der Prüfung der Erforderlichkeit bietet sich die Folgende Methodik an:

## Prüfvoraussetzungen schaffen:

(abgeleitet aus Art. 35 Abs. 7 Buchstabe a) DSGVO)

*Systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von den Verantwortlichen verfolgten berechtigten Interessen*

* Vollständiges Verzeichnis der Verarbeitungen (VVT), das die Angaben nach Art. 30 DSGVO + notwendige Angaben für Informationspflichten und Rechenschaftspflichten, inklusive Angaben zu eigesetzter Technik, technischer Schnittstellen und Software enthält.
* Systematische Beschreibung: Prozessbeschreibungen, soweit personenbezogene Daten unmittelbar oder mittelbar betroffen sind. Eine bestimmte Form ist hier nicht vorgeschrieben. Bei kleineren Verfahren kann auch eine geeignete Veranschaulichung auf Papier erfolgen. Es müssen aber Zugriffsberechtigungen Interner und Externer hervorgehen und ggf. welche Daten betroffen sind.

Die weiteren Mindestanforderungen aus Art. 35 Abs. 7 Buchstaben b) – d) werden erst bei der DSFA geprüft. Buchstabe a) muss vorgezogen werden, weil sonst keine ausreichende Grundlage für die Beurteilung besteht.

## Schwellwertanalyse durchführen

Die Schwellwertanalyse erfolgt nach den Maßstäben in Art. 35 Abs. 1, 3 und 4 DSGVO, wobei in den Fällen von Art. 35 Abs. 3 und 4 DSGVO der Schwellwert stets überschritten und eine DSFA erforderlich ist. Folgende Prüfreihenfolge bietet sich an:

### Schritt 1: Positivliste der Aufsichtsbehörde gemäß Art. 35 Abs. 4 DSGVO:

Fällt eine Verarbeitung unter die Positivliste der Aufsichtsbehörde gemäß Art. 35 Abs. 4 DSGVO, muss stets eine DSFA durchgeführt werden. Der LDI als zuständige Aufsichtsbehörde in NRW veröffentlicht eine Liste für den öffentlichen und nicht-öffentlichen Bereich. Für die öffentlichen Hochschulen ist die Liste des LDI für den öffentlichen Bereich maßgeblich: https://www.ldi.nrw.de/mainmenu\_Aktuelles/submenu\_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Liste-Art-35-4-NRW-OeB\_v2.pdf

**Mögliche Ergebnisse in Schritt 1:**

**Fällt unter die Positivliste:** Eine DSFA ist erforderlich. Gegebenenfalls kann eine größere Verarbeitung in mehrere kleinere Verarbeitungen aufgeteilt werden, um den Bereich für eine erforderliche DSFA zu verkleinern.

**Wenn nein:** Schritt 2

### Schritt 2: Prüfung von Art. 35 Abs. 3 DSGVO

In den folgenden in Art. 35 Abs. 3 DSGVO geregelten Fällen muss stets eines DSFA durchgeführt werden:

1. Bei systematischer und umfassender 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 erheblicher Weise beeinträchtigen*; Erwägungsgrund 71: „insbesondere, wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen.*
2. Bei umfänglicher Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Absatz 1 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO; *Erwägungsgrund 75: wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden*
3. Bei systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche.

**Zur Auslegung gibt der LDI die folgenden Hinweise:**

Hinsichtlich der Größe des Umfangs der Verarbeitung ist nicht nur auf die Zahl der Personen abzustellen, sondern auch auf den Umfang der Angaben.

**Mögliche Ergebnisse in Schritt 2:**

**Voraussetzungen Art. 35 Abs. 3 DSGVO gegeben:** Eine DSFA ist erforderlich. Gegebenenfalls kann eine größere Verarbeitung in mehrere kleinere Verarbeitungen aufgeteilt werden, um den Bereich für eine erforderliche DSFA zu verkleinern.

**Wenn nein:** Schritt 3

### Schritt 3: Andere hochriskante Verarbeitungstätigkeiten

Auch wenn nach den vorgenannten Schritten keine DSFA erforderlich ist, muss im Rahmen der Schwellwertanalyse geprüft werden, ob nach den Kriterien des Art. 35 Abs. 1 DSGVO gegebenenfalls eine andere hochriskante Verarbeitungstätigkeit ausgeübt wird. Beim Begriff des Risikos verweisen die Aufsichtsbehörden auf 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“* der Art. 29 Datenschutzgruppe.

Kriterien zur Einordnung der Verarbeitungsvorgänge:

1. Bewerten oder Einstufen (Scoring)
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung
3. Systematische Überwachung
4. Vertrauliche oder höchst persönliche Daten
5. Datenverarbeitung in großem Umfang
6. Abgleichen oder Zusammenführen von Datensätzen
7. Daten zu schutzbedürftigen Betroffenen
8. Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen
9. Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert

Werden zwei oder mehr der vorgenannten Kriterien durch eine Verarbeitung erfüllt, muss eine DSFA durchgeführt werden. In Einzelfällen kann bereits die Erfüllung eines Kriteriums ausreichen, wenn ein besonders hohes Risiko besteht. Da die Kriterien der Art. 29 Datenschutzgruppe immer noch sehr viel Interpretationsspielraum belassen, ist eine weiter Konkretisierung erforderlich. Die Datenschutzaufsichtsbehörden gehen in informellen Gesprächen davon aus, dass eine DSFA eher die Ausnahme als die Regel sein wird. Dies spricht eher für eine restriktive Auslegung der Kriterien. Dies soll Eingang in weitere Konkretisierung der Kriterien finden. Neben der Konkretisierung sollen Beispiele aus dem Hochschulbereich genannt werden, wobei nicht nur Positiv- sondern auch Negativbeispiele genannt werden sollen, bei deren Vorliegen keine DSFA erforderlich ist. Die Konkretisierung erfolgt auf Basis der folgenden Liste, die durch die Vorarbeit der Ruhr-Universität Bochum durch Dr. Kai-Uwe Loser entstanden ist:

|  |  |
| --- | --- |
| 1. **Verarbeitungen um zu Bewerten oder Einzustufen**, darunter das Erstellen von Profilen und Prognosen, insbesondere auf der Grundlage von *„Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen“* (ErwG 70 und 91 DS-GVO) | Hierfür seien zur Veranschaulichung folgende drei Beispiele genannt:  1) eine Biotechnologieforschung, bei dem man sich zwecks genetischer Tests direkt an Bürger wendet, um die Erkrankungs-/Gesundheitsrisiken abschätzen bzw. prognostizieren zu können,  2) Forschung bei der zum Ausschluss Probanden hinsichtlich bestimmter medizinischer Indikationen untersucht werden.  3) eine Verwendung der BI eines Campus-Management-Systems um nach bestimmten Kriterien nach Studierenden zu suchen, die Merkmale für ein erhöhtes Risiko eines Studienabbruchs aufweisen um diese proaktiv ansprechen zu können. |
| 1. **Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung:** Verarbeitung, auf deren Grundlage für Betroffene Entscheidungen getroffen werden sollen, „*die Rechtswirkung gegenüber natürlichen Personen entfalten*“ oder diese „*in ähnlich erheblicher Weise beeinträchtigen*“ (Art. 35 Abs. 3 lit a). | Die Verarbeitung kann beispielsweise zum Ausschluss oder zur Benachteiligung von Personen führen. Z.B. Plagiatssoftware, oder Verarbeitungen, die die Studienleistung automatisiert beurteilen könnten hier in Frage kommen. Verarbeitungsvorgänge, die keine oder wenige Auswirkungen auf Personen haben, erfüllen nicht dieses spezielle Kriterium.  Die automatische Erstellung von Listen aufgrund derer eine Entscheidung getroffen wird (z.B. Studienplatzbewerbung, Teilnahme an einer zugangsbeschränkten Lehrveranstaltung), erfüllt nicht dieses Kriterium, wenn aufgrund feststehender Kriterien die gleiche Rangfolge auch bei einer manuellen Auflistung herauskäme. Es besteht dann kein spezielles Risiko aufgrund der Automatisierung. |
| 1. **Systematische Überwachung:** Verarbeitungsvorgänge, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben und auf beispielsweise über Netzwerke erfasste Daten oder auf „*eine systematische [...] Überwachung öffentlich zugänglicher Bereiche*“ (Art. 35 Abs. 3 lit. c) zurückgreifen. | Diese Form der Überwachung stellt ein Kriterium dar, weil die personenbezogenen Daten möglicherweise in Situationen erfasst werden, in denen die Betroffenen unter Umständen nicht wissen, wer ihre Daten erfasst und wie die Daten verwendet werden. Darüber hinaus kann es vorkommen, dass die Betroffenen keine Möglichkeit haben, eine solche Verarbeitung ihrer in der Öffentlichkeit (oder in öffentlich zugänglichen Bereichen) erfassten Daten zu verhindern.  **Kameraüberwachung:** Die bloße Installation von Videokameras reicht für eine systematische Überwachung nicht aus. Es reicht somit nicht die Möglichkeit der zufälligen Erfassung von Verhalten von Personen, weil sie sich zufällig in einem überwachten Bereich aufhalten. Es muss sich vielmehr um eine gezielte Maßnahme mit dem Ziel einer Überwachung handeln, wie z.B. die permanente Überwachung eines Arbeitsplatzes oder die umfassende Überwachung durch Kameras in Bereichen, in denen sich Personen nicht nur kurzzeitig aufhalten.  **Keylogger:** Erfassung und Aufzeichnung sämtlicher Tastaturanschläge auf einem Computer.  Umfassende Erfassung der Daten zur Internetnutzung. |
| 1. **Vertrauliche Daten oder höchst persönliche Daten:** Hierzu zählen besondere Kategorien personenbezogener Daten (Art. 9 sowie personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten (Artikel 10). Artikel 9 umfasst folgende Datenarten: 2. Daten über die rassische oder ethnische Herkunft 3. politische Meinungen 4. religiöse oder weltanschauliche Überzeugungen 5. die Gewerkschaftszugehörigkeit 6. genetische Daten und andere biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person 7. Gesundheitsdaten 8. Daten zum Sexualleben oder der sexuellen Orientierung | Hierfür seien als Beispiele zunächst Gesundheitsdaten oder Daten über politische Einstellungen gemeint. Darüber hinaus gibt es weitere Datenkategorien, die zwar nicht in den DS-GVO-Bestimmungen aufgeführt sind, jedoch die möglichen Risiken für die Rechte und Freiheiten von Personen erhöhen können. Diese personenbezogenen Daten gelten als vertraulich (im gängigen Sinne des Wortes), da sie mit häuslichen und privaten Aktivitäten verknüpft sind (wie etwa die elektronische Kommunikation, deren Vertraulichkeit geschützt werden muss), sich auf die Ausübung eines der Grundrechte auswirken (wie etwa Standortdaten, deren Erfassung die Freizügigkeit in Frage stellt) oder die Verletzung derselben mit ernsthaften Konsequenzen für den Alltag des Betroffenen einhergeht (wie etwa Finanzdaten, die für den Zahlungsbetrug missbraucht werden könnten). In dieses Kriterium können auch Daten wie persönliche Dokumente, E-Mails, Tagebücher, Notizen aus E-Readern mit Notizfunktion sowie über Lifelogging-Anwendungen erfasst werden, fallen. |
| 1. **Datenverarbeitung in großem Umfang:** Zwar ist „in großem Umfang“ in der DSGVO nicht definiert, aber Erwägungsgrund 91 liefert einige Hinweise. | Bei der Beurteilung ob ein großer Umfang erreicht wird, sollten folgende Faktoren berücksichtigt werden:   1. Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe; 2. verarbeitete Datenmenge bzw. Breite der unterschiedlichen verarbeiteten Datenelemente; 3. Dauer oder Dauerhaftigkeit der Datenverarbeitung; 4. geographisches Ausmaß der Datenverarbeitung. |
| 1. **Abgleichen oder Zusammenführen von Datensätzen** | Zum Beispiel solcher 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.  Hierzu gehört nicht: Doublettenprüfung bei der Bewerbung und bei der Einschreibung. Es geht nicht über die vernünftigen Erwartungen der Betroffenen hinaus, wenn die Hochschule damit zu verhindern versucht, dass sich Einzelpersonen mit minimalen Abweichungen bei Angaben doppelt bewerben (Bewerbung) oder doppelt als Studierende in der DV geführt werden. |
| 1. **Daten zu schutzbedürftigen Betroffenen** (ErwG 75): Die Verarbeitung dieser Art von Daten stellt ein Kriterium dar, weil zwischen den Betroffenen und dem für die Datenverarbeitung Verantwortlichen ein größeres Machtungleichgewicht vorliegt; d. h. den Personen ist es unter Umständen nicht ohne weiteres möglich, der Verarbeitung ihrer Daten zuzustimmen bzw. zu widersprechen oder ihre Rechte auszuüben. | Als schutzbedürftige Betroffene gelten beispielsweise folgende Bevölkerungs­gruppen:   1. Kinder (bei ihnen kann nicht davon ausgegangen werden, dass sie in der Lage sind, der Verarbeitung ihrer Daten wissentlich und überlegt zu widersprechen bzw. zuzustimmen), 2. Arbeitnehmer (in hohem Umfang/zusammen mit weiteren Merkmalen), 3. Teile der Bevölkerung mit besonderem Schutzbedarf (psychisch Kranke, Asylbewerber, Senioren, Patienten *usw*.) und Betroffene in Situationen, in denen ein ungleiches Verhältnis zwischen der Stellung des Betroffenen und der des für die Verarbeitung Verantwortlichen vorliegt. |
| 1. **Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen**, wie etwa die Kombination aus Fingerabdruck- und Gesichtserkennung zum Zwecke einer verbesserten Zugangskontrolle *usw*. von Personen auswirken und somit eine DSFA obligatorisch machen. | Aus der DS-GVO (Art. 35 Abs. 1, ErwGG 89 und 91) wird deutlich, dass der Einsatz einer neuen Technologie, die „*entsprechend dem jeweils aktuellen Stand der Technik*“ (ErwG 91) als solche einzuordnen ist, der Grund für die Notwendigkeit einer DSFA sein kann. Das liegt daran, dass der Einsatz einer solchen Technologie mit neuartigen Formen der Datenerfassung und -nutzung einhergehen kann, was möglicherweise ein hohes Risiko für die Rechte und Freiheiten von Personen mit sich bringt. Schließlich sind die persönlichen und gesellschaftlichen Folgen, die der Einsatz einer neuen Technologie haben kann, kaum absehbar. Beispielsweise könnten sich einige Anwendungen des „Internet der Dinge“ erheblich auf den Alltag und das Privatleben auswirken.  Internet der Dinge in Verbindung mit umfassenden und neuartigen Methoden der Sensorik, die Datenschutzverletzungen als Seiteneffekte auslösen können. Z.B. soll ein Wärmesensor den Heizbedarf eines Raums bestimmen. Aufgrund der Nähe zu einem Arbeitsplatz und der Technik der Sensorik, können aber auch Rückschlüsse auf die Körpertemperatur einer Person gezogen werden.  **Kein Fall:** Datenbankbasierte Campus-Management-Systeme, auch wenn diese durch BI umfassende Auswertungsmöglichkeiten bietet. Hierbei handelt es sich weder technisch noch organisatorisch um neuartige Ansätze. |
| 1. Fälle, in denen die Verarbeitung an sich *„****die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindert****“* (Artikel 22 und Erwägungsgrund 91). Hierzu zählen Verarbeitungsvorgänge, mit deren Hilfe Betroffenen der Zugriff auf eine Dienstleistung oder der Abschluss eines Vertrags gestattet, geändert oder verwehrt werden soll. |  |

### Vorprüfung zur Schwellwertanalyse

Eine ausführliche Schwellwertanalyse für jede Verarbeitung ist durch die Hochschulen in der Regel personell nicht leistbar. Es wird deshalb eine Vorprüfung zur Schwellwertanalyse vorgeschlagen, in der die fachlich Verantwortlichen, ggf. unterstützt durch die Datenschutzkoordinatoren, eine erste Einschätzung anhand der konkretisierten Kriterien vornehmen.

Ist kein Kriterium einschlägig, erfolgt keine DSFA.

Bestehen Unsicherheiten muss sich der fachlich Verantwortliche an die zuständige Stelle zur weiteren Prüfung wenden.

Eine erweiterte Schwellwertanalyse findet statt, wenn mindestens ein Kriterium nach der Vorprüfung vorliegt.

Da die Entscheidung über das weitere Vorgehen den fachlich Verantwortlichen überlassen wird, stellt sich die Frage der Überprüfung der Einschätzung. Eine generelle Kontrolle ist im Hochschulumfeld nicht leistbar. Werden andererseits überhaupt keine Maßnahmen vorgesehen, besteht die Gefahr eines Organisationsverschuldens, wenn diese Entscheidungen in größerem Maße falsch getroffen werden. Es wird deshalb vorgeschlagen, die fachlich Verantwortlichen auf die Wichtigkeit einer richtigen Einschätzung hinzuweisen und stichprobenhafte Kontrollen anzukündigen.

### Erweiterte Schwellwertanalyse

Bei der erweiterten Schwellwertanalyse sind neben den fachlich Verantwortlichen, der/die Datenschutzbeauftragte, der/die Informationssicherheitsbeauftragte und ggf. das Rechenzentrum zu beteiligen. Nur in dieser Zusammensetzung ist gewährleistet, dass konkret bestehende erhöhte Risiken richtig erkannt werden können. Bezüglich der Dokumentation der Schwellwertanalyse bestehen folgende Anforderungen des LDI (Dokument: Liste für Verarbeitungstätigkeiten nach Art. 35 Abs. 4 DS-GVO:

*„Das Ergebnis der Vorabprüfung (Schwellwertanalyse) und die zugrunde gelegten Einschätzungen der im Zuge der Verarbeitungstätigkeit möglicherweise auftretenden Schäden sowie die resultierende Schwere und Eintrittswahrscheinlichkeit der Risiken sind zu dokumentieren.“*

Die Formulierung des LDI legt nahe, dass die Beurteilung eines hohen Risikos sich nicht nur nach der potentiellen Schadenshöhe, sondern auch nach der Eintrittswahrscheinlichkeit bestimmt. Somit ergeben sich die folgenden inhaltlichen Anforderungen:

* Es müssen die möglichen Schadensszenarien durch die Verarbeitung anhand der Risiken a) – i) bestimmt werden.
* Für jedes Schadensszenario muss der mögliche Schaden und die Eintrittswahrscheinlichkeit des Schadens einfließen. Hierbei sind die bereits vorgesehenen (Standard-) Sicherheitsmaßnahmen zu berücksichtigen. Dieses Vorgehen erinnert an das Vorgehen in der Informationssicherheit bei der Schutzbedarfsanalyse, wo ebenfalls das Risiko anhand des potentiellen Schadens und der Eintrittswahrscheinlichkeit bestimmt wird.

Anhand dieser Anforderungen bietet sich das Vorgehen über eine Matrix an, die für jedes ermittelte Schadensszenario angewendet wird. Diese ersetzt zwar nicht die Einschätzung, kann aber bei der Beurteilung eines hohen Risikos helfen:

**Schadensszenario anhand der Risiken in a)-i): …**

|  |  |  |  |
| --- | --- | --- | --- |
| Schwerer Schaden | Niedrige Wahrsch. | Mittlere Wahrsch. | Hohe Wahrsch. |
| Normaler Schaden | Niedrige Wahrsch. | Mittlere Wahrsch. | Hohe Wahrsch. |
| Geringer Schaden | Niedrige Wahrsch. | Mittlere Wahrsch. | Hohe Wahrsch. |

**Begründung für die Einschätzung der möglichen Schadensintensität und der Wahrscheinlichkeit: …**

**Auswertung:**

* Rot: Es besteht ein hohes Risiko. Gibt es ein weiteres Schadensszenario mit einem hohen Risiko anhand der Risiken a)-i), muss eine DSFA durchgeführt werden.
* Grün: Es besteht kein hohes Risiko.
* Hohe Wahrscheinlichkeit für einen schweren Schaden: Es besteht ein sehr hohes Risiko. IN diesem Fall ist in jedem Fall eine DSFA durchzuführen.

**Mögliche Ergebnisse in Schritt 3**

**Doppeltes hohes oder sehr hohes Risiko:** Eine DSFA ist erforderlich. Gegebenenfalls kann eine größere Verarbeitung in mehrere kleinere Verarbeitungen aufgeteilt werden, um den Bereich für eine erforderliche DSFA zu verkleinern.

**Wenn nein:** Es ist keine DSFA erforderlich! Ende der Prüfung.

# DSFA durchführen

Die inhaltlichen Mindestanforderungen an eine DSFA ergeben sich aus Art 35 Abs. 7 DSGVO. Es muss erfolgen:

1. Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen. 🡪 *Bereits im Rahmen der Schwellwertanalyse erfolgt!*
2. Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck.
   1. *Kann der Zweck gegebenenfalls mit weniger einschneidenden Maßnahmen erreicht werden?*
   2. *Wenn a) nein: Ist das Maß der Grundrechtsbeeinträchtigung durch die Verarbeitung höher zu gewichten als der mit der Verarbeitung verfolgte Zweck? Wenn ja, muss die Verarbeitung unterbleiben.*
3. Eine Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen Personen. 🡪 *Die Risikobewertung erfolgt bereits bei der Schwellwertanalyse. Anderenfalls (Fälle Art. 35 Abs. 3 oder 4 DSGVO, in denen stets eine DSFA durchzuführen ist) müssen Risikoszenarien beschrieben und bewertet werden.*
4. Die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass die Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Im Rahmen der geplanten Abhilfemaßnahmen kann zur Vereinfachung ebenfalls wieder auf die Matrix zurückgegriffen werden. Wurde bei einer ausführlichen Schwellwertanalyse eine Matrix erstellt, bietet sich die Wiederholung der Einschätzung anhand der Matrix unter Berücksichtigung der Abhilfemaßnahmen an:

**Nochmalige Einschätzung unter Berücksichtigung der geplanten Abhilfemaßnahmen:**

|  |  |  |  |
| --- | --- | --- | --- |
| Schwerer Schaden | Niedrige Wahrsch. | Mittlere Wahrsch. | Hohe Wahrsch. |
| Normaler Schaden | Niedrige Wahrsch. | Mittlere Wahrsch. | Hohe Wahrsch. |
| Geringer Schaden | Niedrige Wahrsch. | Mittlere Wahrsch. | Hohe Wahrsch. |

**Begründung für die Einschätzung: …**

**Auswertung:**

* Rot: Es besteht weiterhin ein hohes Risiko. Gibt es trotz der Abhilfemaßnahmen weiter zwei Schadensszenarien mit einem hohen Risiko anhand der Risiken a)-i) oder besteht gar weiterhin eine hohe Wahrscheinlichkeit für einen schweren Schaden, muss eine Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO durchgeführt werden.
* Grün: Es besteht kein hohes Risiko mehr, weil die Abhilfemaßnahmen ein Unterschreiten des Schwellwerts bewirkt haben.

# Hilfsmittel zur DSFA

Es stellt sich die Frage, inwieweit die DSFA durch Hilfsmittel erleichtert werden kann.

Privacy Impact Assessment der CNIL

Hierbei handelt es sich um eine von der französischen Datenschutzaufsichtsbehörde (CNIL) entwickelte Software zur Datenschutz-Folgenabschätzung (PIA-Tool). Begleitende Dokumente in englischer Sprache liegen vor: <https://www.cnil.fr/en/PIA-privacy-impact-assessment-en>

Es kann eine PIA-Software in deutscher Sprache verwendet werden. Hierbei werden Angaben in vier Abschnitten erhoben und strukturiert:

1. Kontext (allgemeine Angaben sowie die personenbezogenen Daten selbst, Lebenszyklus der Daten und Betriebsmittel)
2. Grundlegende Prinzipien (Verhältnismäßigkeit, Notwendigkeit, Rechtsgrundlage, Speicherdauer; Information über Rechte der Betroffenen, Auftragsverarbeiter, Empfänger in Drittländern)
3. Risiken
   1. Aktuelle und geplante Maßnahmen
   2. Unrechtmäßiger Zugriff auf Daten/Unerwünschte Veränderung von Daten/Datenverlust
4. Aktionsplan (Verknüpfung der Angaben)

Durch die Software-Lösung handelt es sich insgesamt um ein sehr strukturiertes Vorgehen, das allerdings keine Anpassung des Vorgehens ermöglicht. Es wird auch ein Sechs-Augen-Prinzip angewendet, wodurch Eingaben erst geprüft oder bestätigt werden müssen, bevor es weiter gehen kann. Dies kann lästig sein, wenn die DSFA von nur einer Person erfasst wird. Es ist jedoch eine Prüfung als Einzelperson möglich, indem die Anforderungen übersprungen werden. Zu jedem Eintrag können manuell Kommentare erfasst werden. Am Ende kann der DSB noch einen Kommentar hinterlegen und eine Meinung von Betroffenen kann erfasst werden. Bereits etablierte Maßnahmen können aus einem Katalog ausgewählt oder manuell erfasst werden. Der Charme liegt somit auch darin, dass das Tool konkrete Maßnahmenvorschläge in Bezug auf ermittelte Gefährdungen vorgibt. Die Daten werden in einem textbasierten, offenen Datenformat abgelegt, können also auch extern weiterbearbeitet werden.

Allerdings geht die Software nur von den Gewährleistungszielen Vertraulichkeit, Verfügbarkeit und Integrität und diesbezüglichen Gefährdungen aus. Hier müsste gegebenenfalls eine Erweiterung der Software oder eine ergänzende manuelle Prüfung der fehlenden Gewährleistungsziele erfolgen. Durch den von den Gewährleistungszielen ausgehenden Ansatz, werden die 9 Kriterien der Art. 29-Gruppe nicht direkt berücksichtigt. Es müsste somit geprüft werden, wie die Kriterien in die Prüfung anhand der Gewährleistungsziele eingebaut werden. Die Aufsichtsbehörden in den Ländern befinden sich zum Teil in Tests des Softwaretools und haben bisher noch keine abschließende Beurteilung verlauten lassen, ob mit dem Tool eine vollständige DSFA durchgeführt werden kann. Zumindest eine Unterstützung wird wohl für möglich gehalten, wenn die fehlenden Aspekte mit ergänzenden Prüfungen sichergestellt werden. Einige Aufsichtsbehörden haben die Auskunft gegeben, dass Anfang 2019 eine Entscheidung der Aufsichtsbehörden zu erwarten ist.

Standard-Datenschutz-Modell des ULD SH/der DSK

Als weitere Unterstützung kommt das Standard-Datenschutz-Modell in Betracht. Eine beispielhafte Durchführung einer Prüfung, ist unter folgender URL verfügbar: <https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf>

Hierbei stellen sich die folgenden Aufgaben:

1. Daten, Systeme, Prozesse müssen identifiziert werden
2. Gewährleistungsziele (datenschutzrechtliche Anforderungen) müssen festgelegt werden
3. Generische Maßnahmen zur Umsetzung des Datenschutzes müssen festgelegt werden

Im Bereich der Risikobewertung werden wenige konkrete Fragen als Beispiele oder Hilfestellung gegeben. Es ist daher eher für Datenschutz-Experten geeignet. Das konkrete Vorgehen ist an keiner Stelle zusammenfassend als Prozessbeschreibung aufgeführt, an der man sich orientiert könnte. Insgesamt handelt es sich somit eher um ein Expertentool, dass somit zu einer Unterstützung der DSFA mit einer breiten Beteiligung von Personen wenig geeignet ist.