Medizinischer Dienst
Nordrhein

Prüfschema zur Frage, ob eine Datenschutz-Folgenabschätzung (DSFA) notwendig ist

Bei der Datenschutz-Folgenabschätzung handelt es sich um eine Regelung nach der Datenschutz-Grundverordnung (DSGVO), bei der die Verantwortlichen der Datenverarbeitung verpflichtet werden, für bestimmte Verfahren, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen.

Die Frage, ob ein Verarbeitungsvorgang die Ausführung einer Datenschutz-Folgenabschätzung erfordert, wird sowohl bei der Einführung als auch bei einer wesentlichen Änderung bestehender Verarbeitungsvorgänge relevant.

Ob eine Datenschutz-Folgenabschätzung notwendig ist, wird im Rahmen einer „Vorprüfung“ geklärt. Das Ergebnis der „Vorprüfung“ (nicht zu verwechseln mit der eigentlichen Durchführungen der Datenschutz-Folgenabschätzung) ist auch dann zu dokumentieren, wenn die oder der Verantwortliche zu der Auffassung gelangt, dass ein Verarbeitungsvorgang nicht folgenabschätzungspflichtig ist.

Folgender Verarbeitungsvorgang wird betrachtet:
Verantwortliche Organisationseinheit:
Ansprechpartner:

Bitte beantworten Sie für die Prüfung und Entscheidung, ob eine Datenschutz-Folgenabschätzung notwendig ist, die nachfolgenden aufgeführten Fragen:

Prüfschritt 1: Rechtliche Voraussetzungen des § 24 Abs. 1, 2 und 3 des Landesdatenschutzgesetz NRW (LDSG NRW)

1.1 Wurde von der fachlich zuständigen obersten Landesbehörde oder von einer durch diese ermächtigte öffentliche Stelle bereits eine, Datenschutz-Folgenabschätzung durchgeführt (§ 24 Abs. 1 LDSG)	Ja ☐	Nein ☐
Erklärung:		

1.2 Wurde von einer obersten Landesbehörde zu dem eingesetzten Verfahren, von ihr oder von einer von ihr ermächtigten Behörde eine durchgeführte Datenschutz-Folgenabschätzung zur Verfügung gestellt (§ 24 Abs. 2 LDSG NRW)?	Ja ☐	Nein ☐
Erklärung:		

1.3 Wurde das automatische Verfahren, das zum Einsatz beim Medizinischen Dienst Nordrhein bestimmt ist, von einer öffentlichen Stelle entwickelt und übernehmen wir dieses im Wesentliche unverändert (§ 24 Abs. 3 LDSG NRW)?	Ja ☐	Nein ☐
Erklärung:		

Ergebnis: Wird eine oder werden mehrere der vorangegangenen Fragen für das zu beurteilende Verfahren mit „Ja“ beantwortet, liegt ein Anwendungsfall nach § 24 des LDSG NRW vor und eine Datenschutz-Folgenabschätzung kann ohne weitere Prüfung unterbleiben. Ansonsten ist mit Prüfschritt 2 fortzufahren.

Prüfschritt 2: „Whitelist“ nach Art. 35 Abs. 5 DSGVO

2.1 Ist der Verarbeitungsvorgang in der „Whitelist“ des Landesbeauftragten für Datenschutz und Informationsfreiheit genannt? Diese „Whitelist“ kann auf der **Homepage** (https://www.ldi.nrw.de/) der datenschutzrechtlichen Aufsichtsbehörde eingesehen werden.	Ja ☐	Nein ☐
Erklärung:		

Ergebnis: Wird die Frage mit „Ja“ beantwortet, kann eine Datenschutz-Folgenabschätzung ohne weitere Prüfung unterbleiben. Wird die Frage mit „Nein“ beantwortet, ist mit Prüfschritt 3 fortzufahren.

Prüfschritt 3: Datenschutz-Folgenabschätzung nach Art. 35 Abs. 1 Satz 2 DSGVO

3.1 Liegt eine Datenschutz-Folgenabschätzung für einen schon bearbeiteten, ähnlichen Verarbeitungsvorgang mit ähnlichen Risiken vor (Art. 35 Abs. 1 Satz 2 DSGVO)?	Ja ☐	Nein ☐
Erklärung:		

Ergebnis: Wird die Frage mit „Ja“ beantwortet, kann die bestehende Datenschutz-Folgenabschätzung für den aktuellen Vorgang genutzt werden. Wird die Frage mit „Nein“ beantwortet, ist mit Prüfschritt 4 fortzufahren.

Prüfschritt 4: Tatbestand nach Art. 35 Abs. 3 DSGVO

4.1 Liegt eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen vor, die auf einer automatisierten Verarbeitung beruht, die als Grundlage für Entscheidungen mit Rechtswirkung dient (Art. 35 Abs. 3 lit. a DSGVO)?	Ja ☐	Nein ☐
Erklärung:		

4.2 Liegt eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten (Art. 9 DSGVO/Art. 35 Abs. 3 lit. b DSGVO) vor?	Ja ☐	Nein ☐
Erklärung:		

4.3 Liegt eine systematische umfangreiche Überwachung im öffentlich zugänglichen Bereich (Art. 35 Abs. 3 lit. c DSGVO) vor?	Ja ☐	Nein ☐
Erklärung:		

Ergebnis: Wird eine oder werden mehrere der vorangegangenen Fragen für das zu beurteilende Verfahren mit „Ja“ beantwortet, liegt ein Tatbestand nach Art. 35 Abs. 3 DSGVO vor und eine Datenschutz-Folgenabschätzung ist notwendig. Ansonsten ist mit Prüfschritt 5 fortzufahren.

Prüfschritt 5: „Blacklist“ nach Art. 35 Abs. 4 DSGVO

5.1 Wird der Verarbeitungsvorgang auf der sogenannten „Blacklist“ der datenschutzrechtlichen Aufsichtsbehörde geführt? Diese „Blacklist“ kann auf der **Homepage** (https://www.ldi.nrw.de/) eingesehen werden.	Ja ☐	Nein ☐
Erklärung:		

Ergebnis: Wurde die vorangegangene Frage mit „Ja“ beantwortet, weil der Verarbeitungsvorgang in einer „Blacklist“ geführt ist, ist eine Datenschutz-Folgenabschätzung notwendig. Wurde die Frage mit „Nein“ beantwortet, ist mit Prüfschritt 6 fortzufahren.

Prüfschritt 6: Bewertungskriterien, ob ein Verarbeitungsvorgang die Wahrscheinlichkeit eines hohen Risikos mit sich bringt.

6.1 Werden im Verarbeitungsprozess personenbezogene Daten mit dem Ziel der Bewertung und Einstufung erhoben? Ja ☐ Nein ☐

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

Erklärung:

6.2 Werden im Verarbeitungsprozess personenbezogene Daten zur automatisierten Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung erhoben? Ja ☐ Nein ☐

Beispiel: 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. 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.

Erklärung:

6.3 Werden im Verarbeitungsprozess personenbezogene Daten zur systematischen Überwachung erhoben? Ja ☐ Nein ☐

Beispiel: 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 zurückgreifen.

Erklärung:

6.4 Werden im Verarbeitungsprozess vertrauliche oder höchst persönliche Daten erhoben? Ja ☐ Nein ☐

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

DSGVO oder Finanzdaten, die umfassende Auskünfte über die finanziellen Verhältnisse zulassen oder für Zahlungsbetrug missbraucht werden können.

Erklärung:

6.5 Werden im Verarbeitungsprozess in großem Umfang personenbezogene Daten erhoben? Ja ☐ Nein ☐

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

- Zahl der Betroffenen, entweder als konkrete Anzahl der Betroffenen oder als Anteil an der entsprechenden Bevölkerungsgruppe;
- verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente;
- Dauer oder Dauerhaftigkeit der Datenverarbeitung;
- geografisches Ausmaß der Datenverarbeitung.

Erklärung:

6.6 Werden im Verarbeitungsprozess personenbezogene Daten zum Abgleichen oder Zusammenführen von Datensätzen erhoben? Ja ☐ Nein ☐

Beispiel: 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.

Erklärung:

6.7 Werden im Verarbeitungsprozess überwiegend personenbezogene Daten von schutzbedürftigen betroffenen Personen erhoben? Ja ☐ Nein ☐

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

Erklärung:

6.8 Werden im Verarbeitungsprozess personenbezogene Daten im Rahmen innovativer Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen erhoben? Beispiel: Hierunter fällt beispielsweise die Kombination aus Fingerabdruck- und Gesichtserkennung zum Zwecke einer verbesserten Zugangskontrolle. Das mögliche Risiko für die Rechte und Freiheiten der Betroffenen kann sich in dieser Fallvariante aus der neuartigen Form der Datenerfassung und Nutzung ergeben. Erklärung:	Ja ☐ Nein ☐

6.9 Werden betroffene Personen im Verarbeitungsprozess an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert? Beispiel: Hierzu zählen beispielsweise Verarbeitungsvorgänge, mit deren Hilfe betroffenen Personen der Zugriff auf eine Dienstleistung gestattet oder verwehrt werden soll. Erklärung:	Ja ☐ Nein ☐

Ergebnis: Wurden im Prüfabschnitt 6 zumindest zwei Fragen mit „Ja“ beantwortet wurden, so ist eine Datenschutz-Folgenabschätzung durchzuführen. Wurden die Fragen mit „Nein“ beantwortet, ist mit Prüfschritt 7 fortzufahren.

Prüfschritt 7: Schwellwertanalyse

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 Datenschutz-Folgenabschätzung 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“.

Eine Datenschutz-Folgenabschätzung ist durchzuführen, wenn eine Risikobewertung ergibt, dass eine Datenverarbeitung ein sehr hohes Risiko (in der Skalierung die roten Felder) für die Betroffenen, deren Daten verarbeitet werden, zur Folge hat.

Ergibt die Risikobewertung, dass eine Datenverarbeitung ein hohes Risiko (in der Skalierung die gelben Felder) für die Betroffenen, deren Daten verarbeitet werden, zur Folge hat, liegt es in dem Ermessensspielraum der verantwortlichen Organisationseinheit, ob eine Datenschutz-Folgenabschätzung durchzuführen ist. Entscheidet sich diese dagegen, ist eine entsprechende Dokumentation inkl. Begründung notwendig.

Die folgende Vorlage zur Erstellung der Risikobeschreibung und –bewertung ist auszufüllen. Zur Hilfestellung ist am Ende des Dokuments ein Beispiel aufgeführt.

1) Eintrittswahrscheinlichkeit

	Risiko	**Bewertung der Eintrittswahrscheinlichkeit (1 = gering 2 = mittel 3 = hoch)**
1		
2		
3		
4		
Mittelwert der Eintrittswahrscheinlichkeit:		0,00

2) Schwere des Schadens (Auswirkung)

	Risiko	**Bewertung der Schwere des Schadens (1 = gering 2 = mittel 3 = hoch)**
1		
2		
3		
4		
Mittelwert der Schwere des Schadens:		0,00

3) Darstellung des Gesamtrisikos

Gesamtrisiko = Mittelwert der Eintrittswahrscheinlichkeit multipliziert mit dem Mittelwert der Schwere des Schadens

Gesamtrisiko = 0,00

Um zu ermitteln, ob eine Datenschutz-Folgenabschätzung notwendig ist, ist das Ergebnis in der folgenden Darstellung des Gesamtrisikos einzutragen.

Schwere des Schadens	hoch (3)	3	6	9
	mittel (2)	2	4	6
	gering (1)	1	2	3
		gering (1)	mittel (2)	hoch (3)
		Eintrittswahrscheinlichkeit		

Wenn keine Datenschutz-Folgenabschätzung erforderlich ist (in der Darstellung die grünen Felder), werden diese beiden Punkte (Durchführung der Risikobewertung und Schwellenwertanalyse) im Verzeichnis von Verarbeitungstätigkeiten dokumentiert.

Ergibt die Risikobewertung, dass eine Datenverarbeitung ein mittleres Risiko (in der Darstellung die gelben Felder) für die Betroffenen, deren Daten verarbeitet werden, zur Folge hat, liegt es in dem Ermessensspielraum der verantwortlichen Organisationseinheit, ob eine Datenschutz-Folgenabschätzung durchzuführen ist. Entscheidet sich diese dagegen, ist eine entsprechende Dokumentation inkl. Begründung notwendig.

Ergibt die Risikobewertung, dass eine Datenverarbeitung ein hohes Risiko (in der Darstellung die roten Felder) für die Betroffenen, deren Daten verarbeitet werden, zur Folge hat, ist eine Datenschutz-Folgenabschätzung durchzuführen.

Beispielberechnung:

1) Eintrittswahrscheinlichkeit

	Risiko	**Bewertung der Eintrittswahrscheinlichkeit (1 = gering 2 = mittel 3 = hoch)**
1	Missbrauchsinteresse	3
2	Aufwand, der nötig ist, um den Schaden herbeizuführen	2
3	Entdeckungsrisiko	2
4	Verarbeitungshäufigkeit	1

Hier ergibt sich als Summe der Bewertung 8. Diese Summe wird durch die Zahl der Kriterien geteilt (in dem Beispiel sind es 4 Kriterien) und es ergibt sich ein **Mittelwert von 2** bei der Eintrittswahrscheinlichkeit.

2) Schwere des Schadens (Auswirkung)

	Risiko	**Bewertung der Schwere des Schadens (1 = gering 2 = mittel 3 = hoch)**
1	Gesundheitliche Auswirkungen	1
2	Finanzielle Auswirkungen	2
3	Soziale Auswirkungen	2
4	Sonstige Auswirkungen (z. B. Ergebnis Pflegeeinstufung wird bekannt)	3

Bei der Schwere des Schadens ergibt sich ebenfalls ein **Mittelwert von 2** (8:4).

3) Gesamtrisiko

Um das Gesamtrisiko zu ermitteln, wird die **Eintrittswahrscheinlichkeit mit der Schwere des Schadens (Auswirkung) multipliziert**, was in dem Beispiel einen **Wert von 4** ergibt.

Um zu ermitteln, ob eine Datenschutz-Folgenabschätzung notwendig ist, ist das Ergebnis in der folgenden Darstellung des Gesamtrisikos einzutragen.

Schwere des Schadens	hoch (3)	3	6	9
	mittel (2)	2	4	6
	gering (1)	1	2	3
		gering (1)	mittel (2)	hoch (3)
		Eintrittswahrscheinlichkeit		

Wenn keine Datenschutz-Folgenabschätzung erforderlich ist (in der Darstellung die grünen Felder), werden diese beiden Punkte (Durchführung der Risikobewertung und Schwellenwertanalyse) im Verzeichnis von Verarbeitungstätigkeiten dokumentiert.

Ergibt die Risikobewertung, dass eine Datenverarbeitung ein mittleres Risiko (in der Darstellung die gelben Felder) für die Betroffenen, deren Daten verarbeitet werden, zur Folge hat, liegt es in dem Ermessensspielraum der verantwortlichen Organisationseinheit, ob eine Datenschutz-Folgenabschätzung durchzuführen ist. Entscheidet sich diese dagegen, ist eine entsprechende Dokumentation inkl. Begründung notwendig.

Ergibt die Risikobewertung, dass eine Datenverarbeitung ein hohes Risiko (in der Darstellung die roten Felder) für die Betroffenen, deren Daten verarbeitet werden, zur Folge hat, ist eine Datenschutz-Folgenabschätzung durchzuführen.

In dem Beispiel ergibt sich für das Gesamtrisiko ein Wert von 4. In der Darstellung des Gesamtrisikos entspricht die 4 einem gelben Feld. Somit liegt es in dem Ermessensspielraum der verantwortlichen Organisationseinheit, ob eine Datenschutz-Folgenabschätzung durchzuführen ist!

Bitte beachten Sie, dass es sich um einen Beispielfall handelt. In Abhängigkeit des Verarbeitungsprozesses sind andere oder zusätzliche Risiken zu bewerten!