

# Hinweise zum Umgang mit der DSFA-Vorlage für das Gesundheitswesen

---

## 1 Allgemeines

Die Vorlage basiert auf der Ausarbeitung von bvitg, DKG und GMDS zur datenschutz-Folgenabschätzung (DSFA), die unter <https://www.gesundheitsdatenschutz.org/html/dsfa.php> in verschiedenen Dateiformaten vorhanden ist.

Die Vorlage besteht aus zwei Teilen:

- 1) Die Word-Datei, in welcher die Beschreibung des Verfahrens sowie andere Angaben aus Art. 35 Abs. 7 DS-GVO aufgenommen werden; die Strukturierung des Dokuments orientiert sich dabei an Kapitel 6 der oben beschriebenen Ausarbeitung
- 2) Einer Excel-Tabelle, in welcher
  - a. Die Erforderlichkeit einer DSFA beurteilt wird,
  - b. die Risiken dargestellt, die Maßnahmen zur Reduzierung der Risiken beschrieben und das Restrisiko beurteilt wird sowie
  - c. der Darstellung der Risikomatrix.

## 2 Word-Datei

(Datei: DSFA-Vorlage\_Gesundheitsversorgung.docx)

Die Word-Datei enthält Textblöcke, die den zu beschreibenden Inhalt verdeutlichen. Grundsätzlich können Inhalte übernommen werden, aber jede DSFA muss zwingend individuell für das jeweilige Szenario der Verarbeitung angepasst werden.

Die Word-Datei ist geschützt, so dass man beim Öffnen zunächst nur die die Formularfelder ausgefüllt werden können. Dabei wurde das Passwort nicht vergeben, so dass jeder die Bearbeitungseinschränkungen aufheben kann.

### Vorgehen zum Aufheben der Bearbeitungseinschränkungen:

Klicken Sie auf der Registerkarte Überprüfen in der Gruppe „Schützen“ auf „Bearbeitung einschr.“, dort das entsprechende Häkchen entfernen

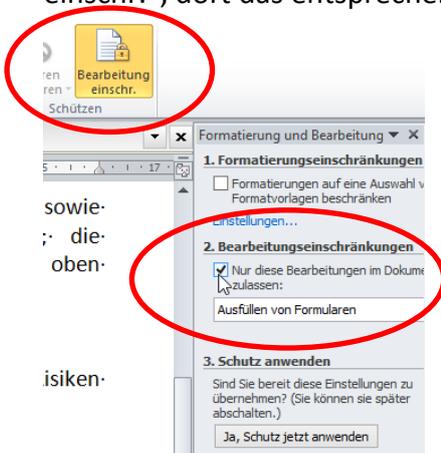


Abbildung 1: Aufheben des Bearbeitungsschutzes in der Word-Datei

## 3 Excel-Tabelle

(Datei: DSFA-Vorlage\_Gesundheitsversorgung\_Risikoanalyse-behandlung.xlsx bzw. als Excel-Vorlage DSFA-Vorlage\_Gesundheitsversorgung\_Risikoanalyse-behandlung.xltx)

Die Excel-Tabelle zeigt beim Öffnen 3 Registerkarten:

- 1) DSFA-Erfordernis  
Hier wird die Erfordernis der DSFA für das konkrete Verfahren dargestellt
- 2) DSFA  
In diesem Tabellenblatt werden alle bekannten Risiken dargestellt sowie die Maßnahmen zur Reduzierung eingetragen. Weiterhin erfolgt die Beurteilung, ob *aus Sicht der betroffenen Personen* das Restrisiko akzeptabel ist oder nicht.
- 3) Risikomatrix  
Die Risikomatrix wird automatisch aus dem Tabellenblatt „DSFA“ berechnet.

### 3.1 Tabellenblatt „DSFA-Erfordernis“

Im Tabellenblatt werden einerseits die Anforderungen aus Art. 35 Abs. 1,3 DS-GVO abgefragt, desgleichen ob die Verarbeitung in der aktuellen (Stand 2019-12-13) Blacklist der deutschen Aufsichtsbehörden gelistet ist. Abhängig von den Antworten auf die einzelnen Fragen ergibt sich eine Erfordernis zur Durchführung einer DSFA oder auch nicht. (siehe Abbildung 2) Dabei werden in den Zeilen 35 bis 37 die Ausnahmetatbestände abgefragt, welche die Erfordernis einer DSFA negieren.

Verarbeitung	Krankenhaus-Informationssystem (KIS) „Complete Recovery“	Datum	21.12.2019
Beurteilung Erforderlichkeit einer Datenschutz-Folgenabschätzung:			
		DSFA nicht erforderlich	
Frage / Prüfung			
Bleibt die Verarbeitung der personenbezogenen Daten ein hohes Risiko für die Rechte und Freiheiten der Betroffenen?			
insbesondere prüfen (mehr als 2 Kriterien legen Vermutung nahe, dass DSFA erforderlich ist):			
Einsatz neuer Verarbeitungstechnologien, d. h. Technologien, zu denen der Verantwortliche noch keine DSFA durchgeführt hat			
Einsatz neuer Verarbeitungen, d. h. Verfahren der Verarbeitung personenbezogener Daten, zu denen der Verantwortliche noch keine DSFA durchgeführt hat			
Verarbeitung großer Datenmengen			
Verarbeitung von Daten einer großen Anzahl betroffener Personen			
Verarbeitungen, welche betroffenen Personen die Wahrnehmung ihrer aus der DS-GVO resultierenden Rechte erschweren			
Soll mit der Verarbeitung die Persönlichkeit des Betroffenen systematisch und automatisiert bewertet werden, sodass rechtliche oder andere intensive Eingriffe für den Betroffenen daraus resultieren bzw. resultieren können?			
Sollen umfangreiche Mengen von Daten, die zu den besonderen Kategorien gehören, verarbeitet werden?			
Sollen umfangreiche Mengen von Daten über strafrechtliche Verurteilungen und Straftaten verarbeitet werden?			
Sollen öffentlich zugängliche Räume überwacht werden?			
Befindet sich die Verarbeitung auf der vom EU Datenschutz-Ausschuss genehmigten Blacklist der nationalen Aufsichtsbehörden?			

Abbildung 2: Erfordernis einer DSFA in Abhängigkeit von den Antworten

Grundsätzlich darf aber immer eine DSFA durchgeführt werden.

### 3.2 Tabellenblatt „DSFA“

Im Tabellenblatt DSFA werden Risiken, Risikoquellen, Maßnahmen usw. als Auswahlfelder abgefragt (siehe Abbildung 3 beispielhaft für Risiken). Die Auswahl der Felder basiert auf Eintragungen auf ausgeblendete Tabellenblätter (siehe Abschnitt 3.4).

Verarbeitungstätigkeit:			
Ifd. Nr.	Risiko-ursprung	Risiken	Risikobeispiele
		nach Erwägungsgrund 83 DS-GVO	
		Bitte Auswahl anklicken	Bitte Auswahl anklicken
0.			
1.	Bitte auswählen	Anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteil	
2.		Auf tauchen (negativer) Informationen (Informationsemergenz)	
3.		Behandlung des Menschen als bloßes Objekt	
		Bildung eines Persönlichkeitsprofils	
		Benutzungsprüfungen, Förderungsmanagement	
		Deutliche Verfügbarkeit (negativer) Informationen	

Abbildung 3: Auswahl von Risiken im Tabellenblatt DSFA

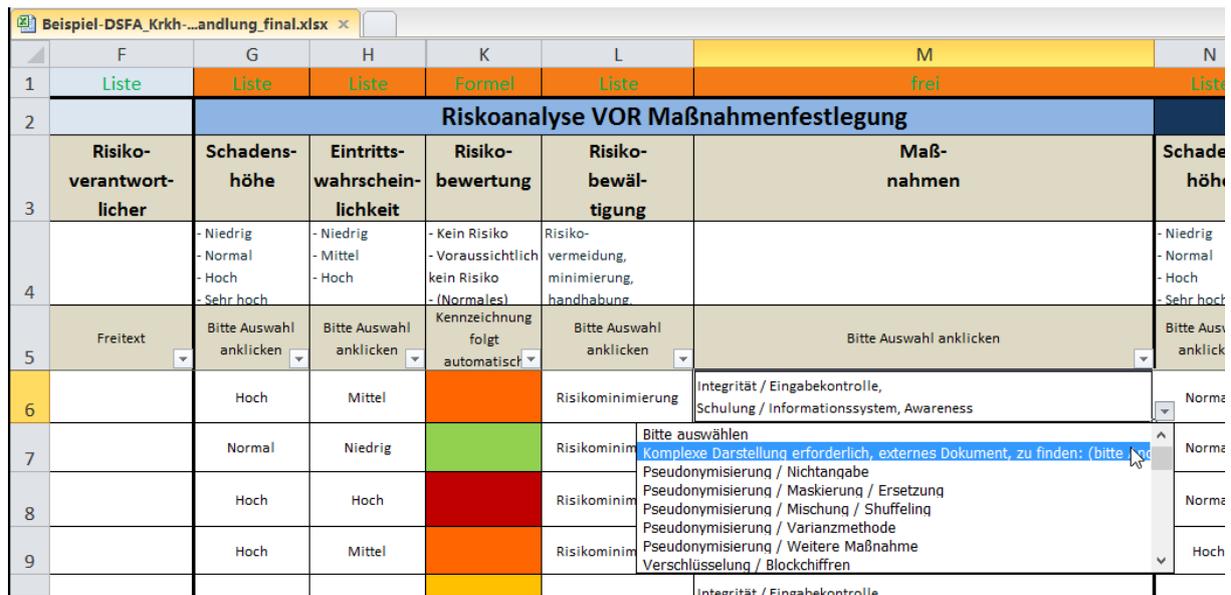
Grundsätzlich können die Felder auch mit Freitext gefüllt werden (siehe Abbildung 4), bei Bedarf kann auch ein Auswahltext mit einem Freitext ergänzt werden.

Verarbeitet			
Ifd. Nr.	Risiko-ursprung	Risiken	
		nach Erwägungsgrund 83 DS-GVO	
		Bitte Auswahl anklicken	
0.		Erringung der Weltherrschaft durch einen übermächtigen Weltkonzern	

Abbildung 4: Eingabe Freitextfeld in tabellenblatt DSFA

Die Risikoanalyse erfolgt einmal vor und einmal nach der Maßnahmenergreifung, damit die Änderungen bei der Risikobetrachtung nachvollziehbar bleiben. Hier sind einige Auswahlfelder vor Freitext geschützt, d. h. es muss auf die vorgegebenen Elemente bei Schadenshöhe und Eintrittswahrscheinlichkeit zurückgegriffen werden; dies dient der automatisierten Auswertung im Feld „Risikobewertung“. Die vorgegebenen Inhalte bei

Schadenshöhe, Eintrittswahrscheinlichkeit und Risikobewältigung entsprechen den Vorgaben der Eingangs erwähnten Ausarbeitung von bvitg, DKG und GMDS und sind nicht änderbar. „Maßnahmen“ hingegen ist wiederum ein Feld, welches sowohl komplett mit Freitext beantwortet werden kann, aber natürlich können auch hier die Auswahltexte durch Freitext ergänzt werden. Da Excel die Anzahl von Zeichen pro Zelle auf 32.767 begrenzt, dies für die Darstellung komplexer Maßnahmen nicht ausreicht, wurde zusätzlich der Hinweis auf eine komplexe Darstellung in einer externen Datei (siehe Abbildung 5) vorgesehen, wobei dann der Speicherort der Datei angegeben werden muss.



	F	G	H	K	L	M	N
1	Liste	Liste	Liste	Formel	Liste	frei	Liste
2	<b>Risikoanalyse VOR Maßnahmenfestlegung</b>						
3	Risiko-verantwortlicher	Schadens-höhe	Eintritts-wahrscheinlichkeit	Risiko-bewertung	Risiko-bewäl-tigung	Maß-nahmen	Schade-höhe
4		- Niedrig - Normal - Hoch - Sehr hoch	- Niedrig - Mittel - Hoch	- Kein Risiko - Voraussichtlich kein Risiko - (Normales)	Risiko-vermeidung, minimierung, handhabung		- Niedrig - Normal - Hoch - Sehr hoch
5	Freitext	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Kennzeichnung folgt automatisch	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Bitte Aus anklick
6		Hoch	Mittel		Risikominimierung	Integrität / Eingabekontrolle, Schulung / Informationssystem, Awareness	Norme
7		Normal	Niedrig		Risikominimierung	Bitte auswählen Komplexe Darstellung erforderlich, externes Dokument, zu finden: (bitte auswählen) Pseudonymisierung / Nichtangabe	Norme
8		Hoch	Hoch		Risikominimierung	Pseudonymisierung / Maskierung / Ersetzung Pseudonymisierung / Mischung / Shuffling Pseudonymisierung / Varianzmethode	Norme
9		Hoch	Mittel		Risikominimierung	Pseudonymisierung / Weitere Maßnahme Verschlüsselung / Blockchiffren	Hoch

Abbildung 5: Eingabemöglichkeit bei der der Risikoanalyse und -behandlung

Die Felder im Bereich „Risikoanalyse NACH Maßnahmenfestlegung“ sind natürlich analog auszufüllen. In der Spalte „U“ („Ergebnis“) stehen „Restrisiko akzeptabel“ und „Weitere Maßnahmen erforderlich“ zur Bewertung des in der jeweiligen Zeile angegebenen Restrisikos zur Auswahl. Lauten alle Bewertungen „Restrisiko akzeptabel“, so ist das Ergebnis der DSFA „Verfahren kann durchgeführt werden“, sollte jedoch nur ein Risiko weitere Maßnahmen erfordern, so wird die DSFA negativ bewertet (siehe Abbildung 6).

Maßnahmen	Ergebnis	Maßnahmen	Ergebnis
	Verfahren kann durchgeführt werden		Weitere Maßnahmen erforderlich, bzw. Aufsichtsbehörde einschalten
Bitte Auswahl anklicken	Bitte Auswahl anklicken	Bitte Auswahl anklicken	Bitte Auswahl anklicken
itenpannen, so dass Betroffenen finanzielle n können	Restrisiko akzeptabel	itenpannen, so dass Betroffenen finanzielle können	Weitere Maßnahmen erforderlich
itenpannen, so dass Betroffenen finanzielle n können	Restrisiko akzeptabel	itenpannen, so dass Betroffenen finanzielle können	Restrisiko akzeptabel

Abbildung 6: Bewertung der DSFA

### 3.3 Tabellenblatt „Risikomatrix“

Im Tabellenblatt wird die Auswirkung der getroffenen Maßnahmen auf das Risiko der Verarbeitung für die betroffenen Personen basierend auf den Angaben im Tabellenblatt „DSFA“ in einer Risikomatrix dargestellt, so dass die Resultate auf einen Blick erkennbar sind.

P	Q	R	S	T	U	V	W
Kein Risiko	x	Eintrittswahrscheinlichkeit	hoch	0	0	1	0
Voraussichtlich kein Risiko	x			0	1	13	1
(Normales) Risiko	x		mittel	0	1	13	1
Erhebliches Risiko	x			0	1	2	0
Hohes Risiko	x			niedrig	0	1	2
Untragbares Risiko	x		niedrig		normal	hoch	sehr hoch
			Schadenshöhe				
<b>Risikomatrix vor Maßnahmenplanung</b>							
Kein Risiko	x	Eintrittswahrscheinlichkeit	hoch	0	0	0	0
Voraussichtlich kein Risiko	x			0	3	0	0
(Normales) Risiko	x		mittel	0	3	0	0
Erhebliches Risiko	x			0	12	1	0
Hohes Risiko	x			niedrig	3	12	1
Untragbares Risiko	x		niedrig		normal	hoch	sehr hoch
			Schadenshöhe				

Abbildung 7; Risikomatrix basierend auf den Angaben im Tabellenblatt DSFA

### 3.4 Ausgeblendete Tabellenblätter

Tabellenblätter, welche „nur“ als Auswahlquelle oder zur Berechnungshilfe dienen, sind ausgeblendet. Ausgeblendete Tabellenblätter sind:

- Riskomatrix2
- Risikoanalyse
- Risiken
- Risikobeispiele
- Risikoquellen
- Risikobewältigung
- Maßnahmen
- Ergebnis
- Risikoberechnung
- Ausfüllhilfen

Die Excel-Tabelle ist nicht passwortgeschützt, so dass jedes Tabellenblatt eingeblendet und die Inhalte an die eigenen Bedürfnisse angepasst werden kann.

Insbesondere bei den Tabellenblättern

- Risiken
- Risikobeispiele

- Risikoquellen
- Maßnahmen

ist dies sogar ausdrücklich erwünscht, denn eine DSFA muss ja die Risiken für die jeweilige Verarbeitung abbilden. Ob man dazu lieber die Möglichkeit zur Freitexteingabe nutzt oder die Auswahlfelder ergänzt, hängt natürlich vom jeweiligen Einzelfall ab.

#### 4 Nachweis der DSFA

Sowohl Word als auch Excel können schnell auch unbeabsichtigt geändert werden. Gerade bei Excel wird ein Auswahlfeld bei einem Nachlesen der Angaben auch schon einmal schnell ungewollt manipuliert, so dass die DSFA danach nicht mehr stimmt.

Um den aus Art. 5 Abs. 2 DS-GVO resultierenden Nachweispflichten zu genügen, wird nach Fertigstellung der DSFA daher die Erzeugung von pdf-Dateien empfohlen. Bei den drei eingblendeten Tabellenblättern wurde der Druckbereich festgelegt, so dass die Ergebnisse bei einem Ausdruck in eine pdf-Datei auch lesbar sind; das Tabellenblatt „DSFA“ wurde dabei auf „DIN A3“ formatiert, da DIN A4 als Format keine Lesbarkeit erzeugte.

#### 5 Abkürzungen

Abs.	Absatz
Art.	Artikel
bvitg	Bundesverband Gesundheits-IT e.V.
DKG	Deutsche Krankenhausgesellschaft e.V.
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Datenschutz-Grundverordnung
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.