Medizinischer Dienst
Nordrhein

Datenschutz-Folgenabschätzung (DSFA)

Zum Verarbeitungsvorgang

laut anliegendem Verarbeitungsverzeichnis

Medizinischer Dienst Nordrhein

Vorbemerkung

Zweck einer Datenschutz-Folgenabschätzung (DSFA) ist es, die personenbezogenen Daten zu schützen, mit denen wir umgehen. Hierzu finden Sie im Rahmen der DSFA etwaige erhebliche Risiken für personenbezogene Daten heraus und können so die notwendigen Maßnahmen ergreifen, um Risiken so weit wie möglich einzudämmen und Schäden zu vermeiden.

Achtung: Eine DSFA ist nur nötig, wenn …

1. Ihre Vorprüfung ergeben hat, dass eine DSFA durchgeführt werden muss!

Diese Vorprüfung führen Sie anhand des Prüfschemas, ob eine DSFA notwendig ist. Die entsprechende Datei finden Sie im MeDiNet unter https://medinet.mdk-nordrhein.local/fileadmin/files/Beauftragte/Datenschutz/Verarbeitungsverzeichnisse/1m_Pruefschema_Datenschutz-Folgenabschaetzung.docx

2. die DSFA noch nicht von dem Gesetz-/ Verordnungsgeber gemacht wurde, der ggf. die Rechtsgrundlage für die Datenverarbeitung geschaffen hat (Art. 35 Abs. 10 DSGVO).

Medizinischer Dienst Nordrhein

Datenschutz-Folgenabschätzung (DSFA)

Bitte beantworten Sie schriftlich die nachfolgenden Fragen.
So haben Sie nicht nur die DSFA durchgeführt, sondern sie auch gleich schon dokumentiert und können die DSFA nachweisen.

A. Basis: Betroffene Personen und Daten, Rechtsgrundlage

Wessen personenbezogene Daten sollen verarbeitet werden?	**Welche Daten sollen verarbeitet werden?** *z.B.: Name, Adresse, Gesundheitsdaten*	**Rechtsgrundlage(n)?** *(Gesetz oder Einwilligung des Betroffenen)*
Versicherten ☐		
Betreuern/Vertretern der Versicherten ☐		
Beschäftigten des Medizinischen Dienstes Nordrhein ☐		
ambulanten Leistungs-erbringern ☐		
stationären Leistungs-erbringern ☐		
Behörden/Krankenkassen ☐		
sonstige ☐		

Medizinischer Dienst Nordrhein

B. Systematische Beschreibung der geplanten Verarbeitungsvorgänge und deren Zwecke (Art. 35 Abs. 7 lit. a DSGVO)

Geplante Verarbeitungsvorgänge (zutreffendes bitte ankreuzen)	Zweck(e)	Falls vorhanden: Berechtigte Interessen des Medizinischen Dienstes Nordrhein an Verarbeitung	Ist die Verarbeitung für den/die Zweck(e) nötig? Ist sie verhältnismäßig?
erheben, erfassen ☐			
organisieren/ordnen ☐			
speichern ☐			
ändern ☐			
auslesen/abfragen ☐			
verwenden ☐			
übermitteln/verbreiten/auf andere Art bereitstellen ☐			
abgleichen ☐			
verknüpfen ☐			
einschränken ☐			
löschen ☐			

Medizinischer Dienst Nordrhein

C. Kontrolle: Einhaltung der Datenschutzgrundsätze bei der Verarbeitung

Info: Zur Verarbeitung zählt nicht nur, Daten zu erfassen und weiterzuleiten, sondern auch das Speichern einschl. des Gespeichert-Lassen.

Alle Grundsätze des Datenschutzes müssen eingehalten werden!

Die Verarbeitung ist …	*(Bitte ankreuzen)*		*Sind Gegenmaßnahmen notwendig? Falls ja, welche geeigneten Gegenmaßnahmen wurden getroffen?*
▪ **rechtmäßig (insbesondere: es gibt eine gesetzliche Grundlage oder die betroffene Person hat eingewilligt)**	Ja ☐	Nein ☐	
▪ **transparent**	Ja ☐	Nein ☐	
▪ **nicht missbräuchlich**	Ja ☐	Nein ☐	
▪ **an einen bestimmten Zweck gebunden, zur Zweckerreichung notwendig und verhältnismäßig (Interessenabwägung)** *Beispiel: Aufbewahrung von Abrechnungen ist in Ordnung, wenn es zur Darlegung bei etwaigen Rechtsstreitigkeiten noch erforderlich ist.*	Ja ☐	Nein ☐	
▪ **auf die Daten beschränkt, die für den Zweck der Verarbeitung nötig sind (Datenminimierung)**	Ja ☐	Nein ☐	

▪ **endlich – es gibt eine Frist, um die Daten zu löschen.**	Ja ☐	Nein ☐	
▪ **vertraulich – die betreffenden Beschäftigten wurden auf die Geheimhaltung verpflichtet.**	Ja ☐	Nein ☐	
▪ **so angelegt, dass die Betroffenenrechte, sofern sie der betreffenden Person zustehen, sicher verwirklicht werden können. Das kann sein: Recht auf …** **- Auskunft über die personenbezogenen Daten** **- Berichtigung und/oder Vervollständigung** **- Einschränkung der Verarbeitung** **- Widerspruch gegen die Verarbeitung** **- Widerruf der Einwilligung in die Verarbeitung** **- Übertragung der Daten**	Ja ☐	Nein ☐	

Medizinischer Dienst
Nordrhein

D. Risikobewertung (Art. 35 Abs. 7 c) und d) DSGVO i. V. m. Art. 35 Abs. 1 DSGVO)

Risiken (es handelt sich hier lediglich um Beispiele)	Negative Folgen, wenn sich das Risiko verwirklicht? Tipp: siehe Anlage 1.	Mögliche Ursachen	Sind Gegenmaßnahmen notwendig?		Ggf. ergriffene Gegenmaßnahmen *(z. B: Zugriffsrechte beschränken)*	Schwere des Schadens, falls sich das Risiko verwirklicht (hoch = 3, mittel = 2, gering = 1)	Eintrittswahrscheinlichkeit (hoch = 3, mittel = 2, gering = 1)	Welche Garantien, Sicherheitsvorkehrungen und Verfahren sichern ggf. den Datenschutz?
☐ **Unbefugte Weitergabe**		☐ Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges	☐ Ja	☐ Nein		☐ hoch ☐ mittel ☐ gering	☐ hoch ☐ mittel ☐ gering	
☐ **Datenverlust einschließlich Datendiebstahl**		☐ Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges	☐ Ja	☐ Nein		☐ hoch ☐ mittel ☐ gering	☐ hoch ☐ mittel ☐ gering	
☐ **Verarbeitung falscher Daten**		☐ Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges	☐ Ja	☐ Nein		☐ hoch ☐ mittel ☐ gering	☐ hoch ☐ mittel ☐ gering	

Unerlaubte Verarbeitung von Gesundheitsdaten oder sonstiger sensibler Daten i. S. d. Art. 9 Abs. 1 DSGVO ☐		Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges ☐	Ja ☐	Nein ☐		hoch ☐ mittel ☐ gering ☐	hoch ☐ mittel ☐ gering ☐	
Offenlegung der Daten an unbefugte Person ☐		Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges ☐	Ja ☐	Nein ☐		hoch ☐ mittel ☐ gering ☐	hoch ☐ mittel ☐ gering ☐	
Enttarnung der hinter pseudonymisierten Daten stehenden Person ☐		Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges ☐	Ja ☐	Nein ☐		hoch ☐ mittel ☐ gering ☐	hoch ☐ mittel ☐ gering ☐	
Profiling (Art. 4 Ziff. 4 DSGVO) ☐		Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges ☐	Ja ☐	Nein ☐		hoch ☐ mittel ☐ gering ☐	hoch ☐ mittel ☐ gering ☐	

Daten ermöglichen die Erfassung/Bewertung sensibler Sachverhalte ☐		Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges ☐	Ja ☐	Nein ☐		hoch ☐ mittel ☐ gering ☐	hoch ☐ mittel ☐ gering ☐	
Aufenthaltsort bestimmbar ☐		Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges ☐	Ja ☐	Nein ☐		hoch ☐ mittel ☐ gering ☐	hoch ☐ mittel ☐ gering ☐	
Unerlaubte Verarbeitung besonders Schutzbedürftiger, z. B. von Beschäftigten ☐		Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges ☐	Ja ☐	Nein ☐		hoch ☐ mittel ☐ gering ☐	hoch ☐ mittel ☐ gering ☐	
☐		Menschl. Fehler ☐ Vorsätzl. Handeln ☐ Techn. Störung/ Ausfall ☐ Sonstiges ☐	Ja ☐	Nein ☐		hoch ☐ mittel ☐ gering ☐	hoch ☐ mittel ☐ gering ☐	
Mittelwert						0,0	0,0	

Medizinischer Dienst Nordrhein

Darstellung des Gesamtrisikos:

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

Gesamtrisiko = 0,00

Um zu ermitteln, ob eine Datenverarbeitung zulässig 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		

Gesamtrisiko:

Hoch:	Die Datenverarbeitung ist unzulässig
Mittel:	Die Datenverarbeitung liegt im Ermessen der verantwortlichen Organisationseinheit
Gering:	Die Datenverarbeitung ist zulässig (mit Umsetzung der ggf. zu treffenden Gegenmaßnahmen)

Medizinischer Dienst Nordrhein

E. Ergebnis DSFA

Die Verarbeitung ist mit Umsetzung der Gegenmaßnahmen zulässig Ja ☐ Nein ☐
Verantwortlich für die Umsetzung ist: _____ **Datum, Unterschrift**

Medizinischer Dienst
Nordrhein

Anlage 1: Schadenszenarien

(Liste ist nicht abschließend, d. h. weitere Szenarien/Schäden/negative Folgen für die Person, um deren Daten es geht, sind möglich.)

- Verlust der Vertraulichkeit der Daten
- Diskriminierung/Mobbing /Rufschädigung
- Identitätsdiebstahl
- Lebensgefahr
- Finanzielle Verluste bis Existenzgefährdung
- subjektives Unbehagen (z. B. Gefühle der Einschüchterung, des Kontrollverlusts, der Überwachung)
- Hinderung/Hemmung, die eigenen Rechte wahrzunehmen
- sonstiges