# Schulungskompendium

Fragen und Antworten zur Datenschutzfolgenabschätzung

# Einführung in das MCSS Schulungskompendium

- Das digitale MCSS Schulungs- und Einweisungssystem basiert auf den jeweils aktuellen Rahmenbedingungen für die Rechtskonformität in medizinischen Einrichtungen. Für die Anwendung der innovativen didaktischen Schulungen gelten folgende Richtlinien.
  - Pro Frage sind etwa 1,5 – 2,0 Minuten aufzuwenden.
  - Zuerst wird die Frage reflektiert und überlegt, welche Antworten gegeben werden können (evtl. mit schriftlichen Notizen).
  - Anschließend werden die Überlegungen/Notizen mit den richtigen Antworten verglichen.
  - Nach ca. 45 Minuten (ca. 20 Fragen und Antworten) sollte eine Konzentrationspause eingelegt werden.
- Die Anwendung wird in MCSS protokolliert und die Anwendungsstatistik gilt als Nachweisdokument für die rechtlichen Audit Anforderungen.

# Datenschutzfolgenabschätzung (DSFA) – Durchführung

# DSFA - Durchführung

Wann ist eine DSFA durchzuführen?

# Wann ist eine DSFA durchzuführen?

Die DSFA ist immer vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen. Auch bereits bestehende Verarbeitungsvorgänge können unter die Pflicht einer DSFA fallen.

**Praxisbeispiel:**

Neues Gesetz DVG – bestehender Prozess Schmerztagebuch

# Wann ist eine DSFA durchzuführen?

Die DSFA erfolgt nicht aus der Sicht von Organisationsprozessen einer Praxis / Klinik, sondern ausschließlich aus der Sicht der betroffenen Personen, Ihrer Personendaten und der damit verbundenen Risiken.

Dies zeigt sich bereits in der empfohlenen Zusammenstellung des interdisziplinären Teams zur Durchführung der DSFA.
(siehe z.B. DSK KP 5  DSFA)

# DSFA - Durchführung

Wie wird die DSFA durchgeführt?

# Durchführung der DSFA Schritt 1

**Team zusammenstellen** (best practice):

- (Vertreter) Verantwortlicher
- Organisation/Prozesssteuerung
- Datenschutzkoordination hausintern & (ext.) Datenschutzbeauftragter
- IT-Administration
- Person aus dem Kreis welcher die Daten verarbeitet
- Betroffene !
- Auftragsverarbeiter
- weitere Dritte

# Durchführung der DSFA Schritt 2

## Erstellung eines Prüfplans

- Erstellung eines Ablauf- und Prüfplans mit Projektmanagement-Methoden
- Ziele
- Meilensteine
- Zuständigkeiten
- Checks

# Durchführung der DSFA Schritt 3

## Festlegung des Beurteilungsumfanges / Identifikation der Prozesse

- Ermittlung der relevanten Prozesse, bei denen Personendaten verarbeitet werden.
- Abgrenzung von nicht relevanten Prozessen
- Ausführliche Prozessbeschreibung
- Dokumentation durch Flussdiagramm
- Dokumentation der beabsichtigten Zwecke
  (z.B. Beschreibung mit BPMN (Business Process Modeling Notation) / ISO9001)

# Durchführung der DSFA Schritt 4

## Identifikation & Einbindung

Das DSFA-Team identifiziert Betroffene und weitere Akteure der Datenverarbeitung.

Diese sind im Zuge der DSFA ggfs. um Stellungnahmen zu bitten oder im Team zu beteiligen.

# Durchführung der DSFA Schritt 5

## Bewertung Notwendigkeit / Verhältnismäßigkeit der Verarbeitung im Bezug zum Zweck

- Bewertung der Verarbeitungsvorgänge ausgehend vom Zweck
- evtl. Missverhältnis zu Beschränkungen / Freiheiten / Rechte der Betroffenen
- Ggfs. Anpassung von Abläufen, genutzte Technologien

# Durchführung der DSFA Schritt 6

## Identifikation der Rechtsgrundlage

Identifikation und genaue Beschreibung der Rechtsgrundlagen der Verarbeitung nach Art. 6 DSGVO, ggf. in Verbindung mit BDSG neu.

(Eine vollständige DSFA hat im Regelfall einen Umfang von 20 bis 30 Seiten und erfordert eine genaue Dokumentation aller Details. Im Falle eines Datenschutzvorfalls zieht eine unzulängliche DSFA sofort ein empfindliches Bußgeld nach sich.)

# Durchführung der DSFA Schritt 6

## Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung

Die Verarbeitung ist nur rechtmäßig wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: z.B.

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen.

# Durchführung der DSFA Schritt 7

## Modellierung der Risikoquellen

Identifizierung von Risikoquellen

- Technische Risikoquellen (z.B. Telekom-Router / Celle)
- Organisatorisch Risikoquellen (Orga-Lücken)
- Menschliche Risikoquellen (Qualifikationsmängel, Schulungsdefizite)
- Externe Risikoquellen (Hacking, Sicherheitslücken im Betriebssystem)

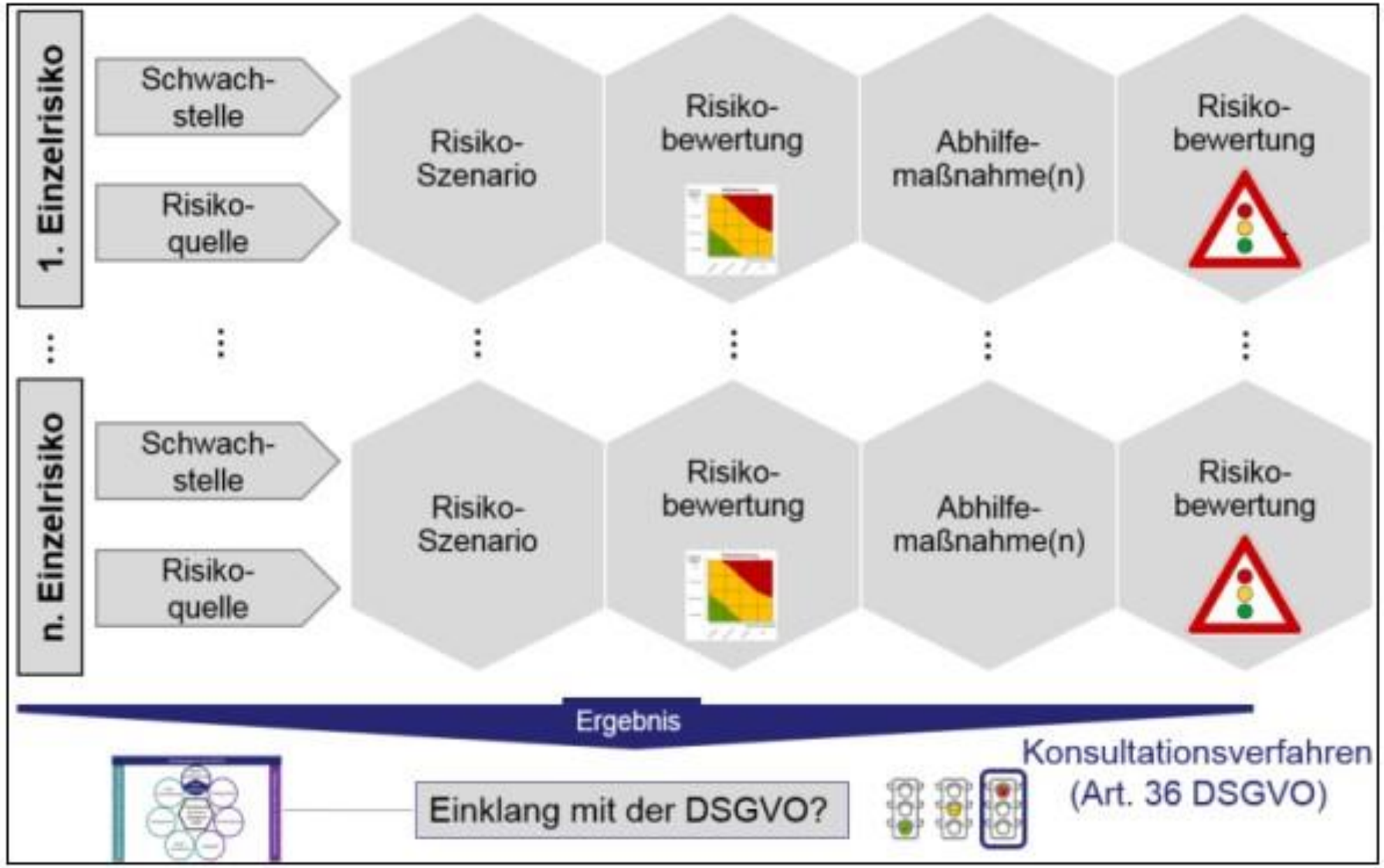


**Abb. 4:** Risikoanalyse der SDM-Datensicherheitsziele

# Durchführung der DSFA Schritt 8

## Risikobeurteilung

Beurteilung der Risiken, welche die Freiheiten und Rechte der Betroffenen einschränken können.

Potenzielle Risiken / eintretende Schäden können physischer, materieller als auch immaterieller Natur sein.

Es ist auch die Schwere und die Eintrittswahrscheinlichkeit zu definieren und auszuwerten.

# Durchführung der DSFA Schritt 9

**Geeignete Abhilfemaßnahmen auswählen**

- Abhilfemaßnahmen basierend auf den ermittelten Risiken
- Die technischen und organisatorischen Maßnahmen (TOM) dämmen mögliche Risiken ein bzw. schließen diese gänzlich aus.

**Verbleibende Restrisiken sind zu ermitteln und zu dokumentieren!**

# Durchführung der DSFA Schritt 10

## Erstellung des Berichtes

1. Einleitung
2. Anwendungsbereich DSFA
3. Datenschutz-Anforderungen
4. Datenschutz-Risikobetrachtung
5. Geplante Abhilfemaßnahmen
6. Ergebnis DSFA und mögliche Pflicht der Konsultation

# Durchführung der DSFA Schritt 11

## Umsetzung der Abhilfemaßnahmen

Die in Pkt. 9 beschriebenen TOM werden umgesetzt und implementiert.

# Durchführung der DSFA Schritt 12

## Test der Abhilfemaßnahmen

Überprüfung der technischen und organisatorischen Maßnahmen:

Sind diese in ausreichendem Maße in der Lage den Schutz der personenbezogenen Daten zu gewährleisten oder müssen noch weitere Anpassungen vorgenommen werden.

# Durchführung der DSFA Schritt 13

## Dokumentation

Umsetzungs- und Testergebnisse werden dem Bericht unter Pkt. 10 hinzugefügt

# Durchführung der DSFA Schritt 14

## Freigabe der Verarbeitungsvorgänge

Sofern die DSFA positiv beendet wurde, kann die Verarbeitung vom Verantwortlichen freigegeben werden.

(Sind die Risiken nicht ausreichend zu beseitigen, so ist die Aufsichtsbehörde zu konsultieren und um Stellungnahme zu bitten! Die Verarbeitung darf bis dahin nicht freigegeben werden.)

# Durchführung der DSFA Schritt 15

## Prüfung / Audit

Um sicherzustellen, das alle TOM in korrekter Form arbeiten, sind regelmäßige Prüfungen zwingend notwendig. Diese sind ohnehin vom Verantwortlichen durchzuführen, sollten aber ergänzend über Audits vom DSB oder eines ext. Dritten neutral überwacht werden.

Die DSFA sollte alle drei Jahre erneut durchgeführt werden.

# Durchführung der DSFA Schritt 15

## Fortschreibung

Änderungen und Anpassungen der geprüften Verarbeitungsvorgänge sind fortzuschreiben. In regelmäßigen Abständen sollten die relevanten Prozesse auf Veränderungen in technischer und organisatorischer Hinsicht überprüft werden. Die Ergebnisse müssen dokumentiert werden.

Die DSFA sollte alle drei Jahre erneut durchgeführt werden.

# DSFA - Durchführung

Was ist zur DSFA zu beachten?
(Zusammenfassung)

# Was ist zur DSFA zu beachten?

**DSFA Zusammenfassung:**

Die DSFA stellt hohe Anforderungen an die Datenschutz-Organisation. Sie sollte in jedem Fall mit Unterstützung eines externen (oder qualifizierten internen) DSB durchgeführt werden.