



STAND

26. September 2026

UNTERLAGE ZUM BEITRAG BRAUCHE ICH EINE DSFA?

Datenschutz-Folgenabschätzung für ein KI-Werkzeug

Mustergliederung für Arztpraxen, mit Vorprüfung und Leitfragen zu jedem Pflichtteil nach Art. 35 Abs. 7 DSGVO

01

Wozu diese Gliederung dient

Die Gliederung hilft einer Praxis, die ein KI-Werkzeug einsetzt oder einführen will, die Datenschutz-Folgenabschätzung aufzubauen. Sie folgt den vier Pflichtteilen aus Art. 35 Abs. 7 DSGVO und stellt davor die Frage, ob eine DSFA überhaupt nötig ist. Zu jedem Teil stehen Leitfragen und Beispiele aus dem Einsatz von KI in der Dokumentation.

Eine DSFA wird je Werkzeug und Einsatz erstellt. Den Rat des Datenschutzbeauftragten holt die Praxis dabei ein (Art. 35 Abs. 2 DSGVO). Viele Angaben für Teil 1 und Teil 4 liefert der Anbieter, am einfachsten über den Anbieterfragebogen KI-Dokumentation auf kleiboldt.de.

02

Vorprüfung: Ist eine DSFA nötig?

Für die gewöhnliche Praxisverwaltung braucht eine Einzelpraxis in der Regel keine DSFA, weil die Verarbeitung von Patientendaten durch einen einzelnen Arzt nicht als umfangreich gilt (Erwägungsgrund 91 DSGVO). Mit einem KI-Werkzeug kann sich das ändern. Drei Fragen klären die Lage.

1. Spricht das Werkzeug selbst mit Patientinnen und Patienten?

Telefonassistent, Chat auf der Website, Terminbot. Die Liste der Datenschutzkonferenz nach Art. 35 Abs. 4 DSGVO nennt unter Nr. 11 den Einsatz künstlicher Intelligenz zur Steuerung der Interaktion mit den Betroffenen. Dann ist eine DSFA durchzuführen.

2. Verarbeitet es Patientendaten, ohne selbst mit Patienten zu sprechen?

Ambient Scribing, Arztbrief- oder Befundentwurf, Auswertung von Dokumenten. Hier kommen Gesundheitsdaten, Patienten als schutzbedürftige Betroffene und eine neue Technologie zusammen. Nach den Leitlinien der europäischen Datenschutzbehörden (WP 248 rev. 01) ist bei zwei oder mehr solchen Kriterien in den meisten Fällen eine DSFA durchzuführen. Die Einschätzung trifft die Praxis im Einzelfall.

3. Arbeitet es ohne Patientendaten?

Praxistexte, Stellenanzeigen, Organisation. Dann ist in der Regel keine DSFA nötig.

Das Ergebnis der Vorprüfung wird mit Begründung festgehalten, auch wenn keine DSFA nötig ist. Ist eine DSFA nötig, braucht die Praxis zugleich einen Datenschutzbeauftragten, unabhängig von ihrer Größe (§ 38 Abs. 1 Satz 2 BDSG).

03

Teil 1: Beschreibung der Verarbeitung

Art. 35 Abs. 7 lit. a DSGVO. Was geschieht mit welchen Daten, wozu und wer ist beteiligt.

Werkzeug. Name, Anbieter mit Rechtsträger, Version, Modul. Zweckbestimmung des Herstellers im Wortlaut und die Angabe, ob es ein Medizinprodukt ist.

Zweck. Welche Aufgabe übernimmt das Werkzeug, zum Beispiel den Entwurf der Behandlungsdokumentation aus dem Gespräch.

Rechtsgrundlage. Für Behandlung und Dokumentation Art. 9 Abs. 2 lit. h DSGVO in Verbindung mit § 22 Abs. 1 Nr. 1 lit. b BDSG. Für die Aufnahme des

Gesprächs das vorher eingeholte Einverständnis, tragender Grund ist § 201 StGB.

Betroffene. Patientinnen und Patienten, Begleitpersonen, Beschäftigte.

Daten. Audio, Transkript, Entwurf, Metadaten wie Zeitpunkt und Nutzerkennung.

Datenweg. Von der Aufnahme über die Verarbeitung beim Anbieter bis in die Praxissoftware, mit Ort der Verarbeitung und Speicherung.

Beteiligte. Anbieter, Unterauftragsverarbeiter mit Sitz und Leistung, C5-Testat des Anbieters nach § 393 SGB V.

Zugriff in der Praxis. Wer nutzt das Werkzeug, wer sieht Entwürfe, wer gibt frei.

Speicherdauer. Löschfristen für Audio, Transkript und Entwurf beim Anbieter und in der Praxis.

04

Teil 2: Notwendigkeit und Verhältnismäßigkeit

Art. 35 Abs. 7 lit. b DSGVO. Die Bewertung nimmt die Praxis mit ihrem Datenschutzbeauftragten vor. Leitfragen:

Welchen Zweck erfüllt das Werkzeug, und erreicht ein milderes Mittel ihn ebenso, etwa das Diktat oder ein Entwurf aus der vorhandenen Dokumentation ohne Aufnahme?

Werden nur die Daten verarbeitet, die für den Zweck nötig sind? Bleibt Audio länger als für die Übertragung nötig erhalten?

Wie werden Patientinnen und Patienten informiert (Art. 13 DSGVO), und was geschieht, wenn jemand die Aufnahme ablehnt?

Wie können Betroffene ihre Rechte ausüben, etwa Auskunft und Löschung, und wie wirkt ein Widerruf des Einverständnisses?

Ist ausgeschlossen, dass der Anbieter die Daten für eigene Zwecke nutzt, oder wer in der Praxis dürfte das freigeben?

05

Teil 3: Risiken für die Patientinnen und Patienten

Art. 35 Abs. 7 lit. c DSGVO. Zu jedem Risiko werden Eintrittswahrscheinlichkeit und Schwere eingeschätzt, jeweils gering, mittel oder hoch.

Unbefugte Kenntnisaufnahme durch Beschäftigte des Anbieters oder eines Unterauftragsverarbeiters.

Zugriff aus einem Drittland über den Anbieter, einen Konzernteil oder den Support.

Falscher oder erfundener Inhalt im Entwurf, der ungeprüft in die Akte gelangt.

Aufnahme ohne Einverständnis oder ohne Information der Anwesenden.

Nutzung für fremde Zwecke, etwa Modelltraining ohne Regel in der Praxis.

Fehlende Löschung von Audio oder Transkript beim Anbieter.

Falscher Zugriff in der Praxis, etwa über geteilte Konten oder offene Geräte.

Ausfall oder Insolvenz des Anbieters mit Daten, die nicht mehr herauszubekommen sind.

06

Teil 4: Maßnahmen

Art. 35 Abs. 7 lit. d DSGVO. Jedem Risiko aus Teil 3 wird mindestens eine Maßnahme zugeordnet, mit Zuständigkeit und Nachweis.

Anbieter. Aktuelles C5-Testat und umgesetzte Kriterien für Kunden, Verpflichtung auf die Schweigepflicht nach § 203 Abs. 4 StGB bis zum letzten Unterauftragnehmer, Auftragsverarbeitungsvertrag mit Gesundheitsdaten als Datenkategorie.

Zwecke. Nutzung für Training und Produktverbesserung vertraglich ausgeschlossen oder in der Praxis ausdrücklich geregelt.

Löschung. Löschfristen als Zahlen im Vertrag, eigener Export der Dokumentation in der Praxissoftware.

Patientinnen und Patienten. Information nach Art. 13 DSGVO, Einverständnis zur Aufnahme vor dem Gespräch, Weg ohne Aufnahme für alle, die ablehnen.

Prüfung. Jeder Entwurf wird vor der Übernahme in die Akte ärztlich geprüft

und freigegeben, die Freigabe wird protokolliert.

Zugriff. Eigene Konten je Person, Rechte nach Rolle, gesperrte Geräte.

Team. Einweisung mit den Unterlagen des Anbieters als Maßnahme zur KI-Kompetenz nach Art. 4 KI-Verordnung, dokumentiert.

Vorfälle. Meldeweg für Datenschutzverletzungen (Art. 33 DSGVO) und ein eingeübter Weg ohne das Werkzeug.

07

Teil 5: Ergebnis, Abzeichnung, Wiedervorlage

Restrisiko. Wie hoch ist das Risiko nach den Maßnahmen? Bleibt es hoch, konsultiert die Praxis vor dem Einsatz die Aufsichtsbehörde (Art. 36 DSGVO).

Stellungnahme des Datenschutzbeauftragten mit Datum (Art. 35 Abs. 2 DSGVO).

Entscheidung der Praxisleitung mit Datum und Unterschrift.

Wiedervorlage. Ein fester Termin, etwa jährlich, und zusätzlich bei jeder Änderung, die das Risiko verändert, zum Beispiel ein Update mit neuen Funktionen (Art. 35 Abs. 11 DSGVO).

Handelt es sich um ein Hochrisiko-KI-System nach der KI-Verordnung, nutzt die Praxis für die DSFA die Informationen aus der Betriebsanleitung des Anbieters (Art. 26 Abs. 9 KI-Verordnung).

Hinweis. Diese Gliederung ist eine allgemeine Unterlage und keine Rechtsberatung im Einzelfall. Für die rechtliche Prüfung und die Gestaltung im Einzelfall binde ich eine Fachanwältin für Datenschutz- und IT-Recht ein.