

Zehnerregel für Schwellwertanalyse der DSFA: Arbeitshilfe für Datenschutzbeauftragte

Diese Arbeitshilfe erläutert die sogenannte Zehnerregel für die Schwellwertanalyse nach SDM-Methode 3.1 D3.2.1. Datenschutzbeauftragte erhalten strukturierte Prüfschritte zur Vorprüfung der DSFA-Pflicht mit Muss-Liste und den neun offiziellen EDSA-Kriterien.

Struktur für Sicherheit. Klarheit für KI.

Zielgruppe: Datenschutzbeauftragte

Stand August 2026

ORIENTIERUNG

Worum es geht

Die Zehnerregel strukturiert die Schwellwertanalyse für DSFA-Vorprüfungen. Sie basiert auf der Muss-Liste der DSGVO und neun EDSA-Kriterien. Diese Arbeitshilfe bietet klare Prüfschritte mit Entscheidungshilfen, Visualisierungsmatrix und transparentem Prüfverfahren. Keine künstlichen Kriterien.

NAVIGATOR

Drei Orientierungspunkte

9

Offizielle
EDSA-Kriterien in der
Analyse

2

Kriterien für
DSFA-Pflicht meist
ausreichend

0

Zehnerregel' im
offiziellen SDM
erwähnt

CHECKLIST

Schritt 1: Muss-Liste der DSGVO prüfen

Starte mit der Muss-Liste gem. Art. 35 Abs. 3 und 4 DSGVO. Prüfe, ob dein Vorhaben DSFA-pflichtige Verarbeitung umfasst.

- Art. 35 Abs. 3 DSGVO: Drei DSFA-pflichtige Arten identifizieren.
- Art. 35 Abs. 4 DSGVO: Nationale Fachlisten der Behörde berücksichtigen.
- Dokumentiere Ausschluss, falls keine Muss-Verarbeitung vorliegt.
- Notiere Arbeitsergebnis zur DSFA-Pflicht abschließend.

CHECKLIST

[] Muss-Liste prüfen
Gesetzliche Muss-Liste prüfen, um DSFA direkt auszulösen.

[] Drei Verarbeitungsarten
Systemüberwachung, automatisierte Entscheidung, sensible Daten.

[] Fachliste kontrollieren
Nationale Aufsichtslisten ergänzend prüfen.

MERKSATZ

Vorrangig immer mit Muss-Liste starten, sie ist Basis vor EDSA-Kriterien.

MATRIX

Schritt 2: Die Neun EDSA-Kriterien für die Schwellwertanalyse (Zehnerregel")

Nach Ausschluss der Muss-Liste folgen die neun EDSA-Kriterien. Die Zehnerregel meint diese Kombination - zehn Prüfgründe liegen faktisch nicht vor.

- Alle neun EDSA-Kriterien einzeln erfassen und dokumentieren.
- Zwei erfüllte Kriterien führen meist zur DSFA-Pflicht.
- Auch ein einziges Kriterium kann je nach Kontext DSFA-Pflicht begründen.
- Keine zusätzlichen, erfundenen Kriterien einbeziehen.

MATRIX

Neun Kriterien

Vollständige Einzelprüfung jedes EDSA-Punktes.

Zählweise offenlegen

Kriterienanzahl sind neun, Begriff Zehnerregel ist Praxisjargon.

DSFA-Pflicht prüfen

Ab zwei erfüllten Kriterien meist DSFA nötig; Kontext zählt.

MERKSATZ

Nur die offiziellen neun EDSA-Kriterien und Muss-Liste fachlich korrekt dokumentieren.

CHECKLIST

Schritt 3: Die Neun EDSA-Kriterien im Detail

Die neun EDSA-Kriterien dienen der systematischen Risikoidentifikation für die DSFA-Vorprüfung.

1 Bewertung/Scoring: Profiling und Einstufung von Personen.

6 Abgleich verschiedener Quellen: Zusammenführung von Datenbeständen.

2 Automatisierte Entscheidung: Entscheidungswirkung für Betroffene.

7 Schutzbedürftige Gruppen: Kinder, Patienten, Beschäftigte.

3 Systematische Überwachung: z. B. Videoüberwachung öffentlicher Räume.

8 Innovative Technologien: KI, maschinelles Lernen, neue Nutzungskonzepte.

4 Vertrauliche Daten: Gesundheitsdaten, religiöse Angaben, Biometriedaten.

9 Rechtehinderung: Einschränkung von Betroffenenrechten, etwa durch Blacklisting.

5 Großer Umfang: Hohe Anzahl Datensätze/Beteiligte.

MERKSATZ

Alle neun Kriterien müssen geprüft und nachvollziehbar dokumentiert werden.

FOCUS

Schritt 4: Kontextanalyse und Dokumentation

Im Einzelfall muss bewertet werden, wie Art, Umfang, Umstände und Zweck jedes Kriterium beeinflussen.

- Jedes relevante Kriterium muss im Verfahrenskontext bewertet werden.
- Risikoabschätzung anhand Art, Umfang, Umstände, Zweck dokumentieren.
- Leitfragen z. B. aus EDSA-Leitlinien zur Risikoermittlung nutzen.
- DSFA-Pflicht oder Verneinung schriftlich und begründet festhalten.

FOCUS

01 Risiko im Zusammenhang
Jede Verarbeitung im Einzelfall bewerten.

02 Dokumentation
Alle Abwägungen und Entscheidungen schriftlich belegen.

03 Leitlinien beachten
Anerkannte Verlautbarungen für Risikoanalyse berücksichtigen.

MERKSATZ

Kontextanalyse ist erforderlich, Zahlen allein reichen nicht als Entscheidungsgrund.

TIMELINE

Schritt 5: Entscheidungsfindung, Dokumentation und Weiterverarbeitung

Ergebnisse der Schwellwertanalyse muss die zuständige Stelle eindeutig dokumentieren und für Aufsichtsbehörden prüfbar halten.

- Arbeitsergebnis zur DSFA-Pflicht ausführlich mit Begründung dokumentieren.
- Prüfen, ob Durchführung oder bloße Feststellung der DSFA notwendig ist.
- Entscheidung an relevante Stellen kommunizieren, negatives Ergebnis begründen.
- Verfahren regelmäßig auf Aktualität und Änderungen überprüfen.

TIMELINE

- **Ergebnisübersicht**
Kurzfassung und Archiv aller Prüfergebnisse.
- **Prüffähigkeit**
Vollständige Nachvollziehbarkeit für Kontrollen ermöglichen.
- **Regelmäßige Review**
Verfahren regelmäßig auf neue Risiken prüfen.

MERKSATZ

Arbeitsergebnisse nachvollziehbar dokumentieren und turnusmäßig prüfen.

MUSTERBEISPIEL

Musterbeispiel: Schwellwertanalyse eines neuen KI-Tools im HR-Bereich

AUSGANGSLAGE

Personalabteilung prüft ein KI-gestütztes System zur automatisierten Bewerberauswahl und Leistungsbewertung.

- 1 Muss-Liste (Art. 35 Abs. 3): Keine direkte DSFA-Pflicht festgestellt.
- 2 EDSA-Kriterien: Profiling, automatisierte Entscheidung, großer Umfang erfüllt.
- 3 Kontextanalyse: Viele Bewerberdaten, unmittelbare Auswirkung auf Auswahlentscheidungen.
- 4 Entscheidung schriftlich dokumentiert und DSFA-Pflicht begründet.
- 5 DSFA vollständig nach Schwellwertanalyse erstellt.

ERGEBNIS

Das Verfahren erfüllt nachweislich mehrere EDSA-Kriterien. Kontextprüfung bestätigt DSFA-Pflicht. DSFA-Bericht wird dokumentiert und archiviert.

ARBEITSBLATT

Umsetzungsscheckliste

- ☐ Muss-Liste gem. Art. 35 Abs. 3/4 DSGVO vollständig geprüft?
- ☐ Liegt eine nationale DSFA-Fachliste vor und wurde sie beachtet?
- ☐ Wurden alle neun EDSA-Kriterien einzeln bewertet?
- ☐ Sind erfüllte Kriterien klar mit Beispielen belegt?
- ☐ Ist eine Kontextanalyse (Art, Umfang, Umstände, Zweck) erfolgt?
- ☐ Erfüllen mindestens zwei EDSA-Kriterien das Risikoschwellenmaß?
- ☐ Wurde die DSFA-Pflicht und ihr Grund dokumentiert?
- ☐ Sind Entscheidungsgründe für/gegen DSFA sauber erläutert?
- ☐ Ist das Ergebnis prüffähig, nachvollziehbar archiviert und zugänglich?
- ☐ Ist ein Wiederholungsintervall für das Verfahren definiert?
- ☐ Wurden keine zusätzlichen Kriterien erfunden oder übernommen?
- ☐ Auf abweichende Zählweise der Zehnerregel transparent hingewiesen?

Nächster Schritt

Die Zehnerregel (real: Muss-Liste + 9 EDSA-Kriterien) bietet Struktur für die Schwellwertanalyse. Eine klar dokumentierte, kontextbasierte Prüfung erleichtert den DSFA-Nachweis und die Kommunikation mit Aufsichtsbehörden.

WEITERFÜHRENDE ORIENTIERUNG

Gesetzesbibliothek · KI-Risikobibliothek · DAXAIS Academy

www.daxais.de