

DSFA-Vorlage — DSGVO Artikel 35

Vorprüfung · Beschreibung · Notwendigkeit & Verhältnismäßigkeit · Risikomatrix · Freigabe · KI-Annex

KOSTENLOSE VORLAGE — DOCX · PDF · MD | Version 1.0 · Stand 2026-07-22

VOR Beginn der Verarbeitung ausfüllen (Art 35(1)).

Die Abschnitte 4–11 tragen den Pflichtinhalt nach Art 35(7)(a)–(d).

Wo ein DSB benannt ist, ist sein Rat verpflichtend (Art 35(2)).

Hohes Restrisiko → zuerst die Aufsichtsbehörde konsultieren (Art 36: 8 Wochen + 6).

Überprüfung spätestens bei veränderter Risikolage (Art 35(11)).

1. Dokumentenkontrolle

DSFA-Referenz	Interne ID, z. B. DPIA-2026-004
Name der Verarbeitung / Funktion	Kurzname der zu bewertenden Verarbeitung
Verantwortlicher / erstellende Person	Juristische Person; Person, die diese DSFA erstellt
Datum Beginn / Freigabe	Lebenszyklus-Daten

2. Vorprüfung — ist eine DSFA erforderlich?

2a. Immer-DSFA-Fälle des Artikels 35(3)

Fall	Trifft zu?
35(3)(a) Systematische und umfassende automatisierte Bewertung/Profiling mit Rechtswirkung oder ähnlich erheblicher Beeinträchtigung	Ja / Nein
35(3)(b) Umfangreiche Verarbeitung besonderer Kategorien (Art 9) oder strafrechtlicher Daten (Art 10)	Ja / Nein
35(3)(c) Systematische umfangreiche Überwachung eines öffentlich zugänglichen Bereichs	Ja / Nein

2b. Die neun Hochrisiko-Kriterien der WP248 rev.01 (Faustregel: zwei erfüllt → DSFA)

Kriterium	Erfüllt?
1. Bewerten oder Einstufen (inkl. Profiling, Vorhersagen)	Ja / Nein
2. Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich erheblicher Wirkung	Ja / Nein
3. Systematische Überwachung	Ja / Nein
4. Vertrauliche oder höchstpersönliche Daten	Ja / Nein
5. Datenverarbeitung in großem Umfang	Ja / Nein
6. Abgleich oder Zusammenführung von Datensätzen	Ja / Nein
7. Daten schutzbedürftiger betroffener Personen	Ja / Nein
8. Innovative Nutzung / neue technische oder organisatorische Lösungen (inkl. KI)	Ja / Nein
9. Verarbeitung, die die Ausübung eines Rechts oder die Nutzung eines Dienstes/Vertrags verhindert	Ja / Nein

Prüfen Sie außerdem die Art-35(4)-Liste Ihrer Aufsichtsbehörde — z. B. die Muss-Liste der DSK (DE), die 14-Kategorien-Liste der CNIL (FR), die UK-Hochrisiko-Liste der ICO, die norwegische Liste des Datatilsynet.

3. Ergebnis der Vorprüfung

DSFA erforderlich?	Ja / Nein — mit den Auslösern: Fall des Art 35(3), Zahl der erfüllten WP248-Kriterien oder Eintrag einer Art-35(4)-Liste
--------------------	--

Falls nein	Begründung dokumentieren und dieses Dokument aufbewahren; erneut prüfen, wenn sich die Verarbeitung ändert
------------	--

4. Systematische Beschreibung der Verarbeitung (Art 35(7)(a))

Art, Umfang, Umstände, Zwecke	Was die Verarbeitung tut, für wen, in welchem Umfang und warum
Kategorien personenbezogener Daten	Besondere Kategorien (Art 9) ausdrücklich kennzeichnen
Kategorien betroffener Personen	Schutzbedürftige Gruppen kennzeichnen (Kinder, Beschäftigte, Patienten)
Empfänger	Interne Teams, Auftragsverarbeiter, Dritte
Drittlandtransfers	Drittländer + Transfermechanismus (SCC, Angemessenheit)
Speicherdauer	Frist und Löschauslöser
Systeme und Datenflüsse	Wo die Daten liegen und sich bewegen
Verfolgtes berechtigtes Interesse	Nur, wenn Art 6(1)(f) herangezogen wird

5. Konsultationsnachweis (Art 35(2), 35(9))

Rat des DSB	Pflicht, wo ein DSB benannt ist — Rat und Datum protokollieren
Standpunkt der betroffenen Personen	Wo angemessen; falls nicht eingeholt, Grund dokumentieren
Konsultierte Auftragsverarbeiter / Anbieter	Z. B. geprüfte Dokumentation des KI-Anbieters

6–7. Notwendigkeit und Verhältnismäßigkeit (Art 35(7)(b))

Rechtsgrundlage	Grundlage nach Art 6; Art-9-Bedingung bei besonderen Kategorien
Notwendigkeit	Warum diese Verarbeitung den Zweck erreicht; angewandte Datenminimierung
Verhältnismäßigkeit	Geprüfte weniger eingriffsintensive Alternativen und warum sie nicht genügen
Transparenz & Rechte	Wie die Betroffenen informiert werden; wie Auskunft, Löschung, Widerspruch und Übertragbarkeit gewährleistet werden

8–10. Risikobewertung (Art 35(7)(c))

Risiken für die Rechte und Freiheiten der betroffenen Personen — keine Unternehmensrisiken. Bewerten Sie Eintrittswahrscheinlichkeit × Schwere auf einer 3×3-Matrix.

	Schwere: Niedrig	Schwere: Mittel	Schwere: Hoch
Wahrscheinlichkeit: Hoch	Mittel	Hoch	Hoch
Wahrscheinlichkeit: Mittel	Niedrig	Mittel	Hoch
Wahrscheinlichkeit: Niedrig	Niedrig	Niedrig	Mittel

Ausgearbeitete Beispielzeile:

ID	Risiko	W	S	Maßnahme	Restrisiko
EX1	Unbefugter Zugriff auf KI-Logs des Kundensupports mit personenbezogenen Daten	M	H	Zugriff auf die Bereitschaftsrolle im Support beschränkt; Logs nach 24 h pseudonymisiert; Speicherfrist auf 30 Tage verkürzt; Zugriffe auditiert	Niedrig

11. Abhilfemaßnahmen (Art 35(7)(d))

Eine konkrete Maßnahme je Risiko. Generische Aussagen senken keine Werte; konkrete TOMs (Art 32), Zugriffskontrollen, Pseudonymisierung und kürzere Speicherfristen schon.

12. Restrisiko & Artikel-36-Entscheidung

Gesamtrestrisiko	Niedrig / Mittel / Hoch — nach allen Maßnahmen
Vorherige Konsultation erforderlich?	Bleibt das Restrisiko HOCH: Konsultieren Sie die Aufsichtsbehörde VOR der Verarbeitung (Art 36) — schriftliche Empfehlung binnen 8 Wochen, verlängerbar um 6
Behörde konsultiert / Antwort	Datum, Referenz, Ergebnis — oder n/a

13–14. Freigabe & Überprüfungsprotokoll (Art 35(2), 35(11))

Freigabe des Verantwortlichen	Name, Funktion, Datum
DSB-Stellungnahme protokolliert	Ja / Nein — Datum
Überprüfungsauslöser	Neue Datenkategorie, neues KI-Modell, neuer Empfänger, neuer Zweck
Nächste geplante Überprüfung	Datum

KI-Annex — KI/LLM-Funktionen und die EU-KI-Verordnung

Für jede KI-gestützte Verarbeitung ausfüllen (WP248-Kriterium 8, typischerweise plus 1, 2 und 5). Für Hochrisiko-KI-Systeme, bei denen Sie Betreiber im Anwendungsbereich des Art 27 der EU-KI-Verordnung sind, kann die FRIA gemeinsam mit dieser DSFA dokumentiert werden — keine Bewertung ersetzt die andere.

Modell / System	Anbieter, Modell, Version
Herkunft der Trainingsdaten	Personenbezogene Daten in Trainings-/Fine-Tuning-Daten? Anbieterdokumentation geprüft?
Automatisierte Entscheidungen & Wirkungen	Rechtswirkung oder ähnlich erhebliche Wirkung (Art 22 DSGVO)? Mensch in der Schleife?
Erklärbarkeit & Aufsicht	Können Ergebnisse den Betroffenen erklärt werden? Welche Aufsichtsmaßnahmen gelten?
Bias-/Genauigkeitsrisiken	Durchgeführte Tests; bekannte Fehlermodi; Monitoring-Plan
Einstufung nach EU-KI-Verordnung	Verboten / Hochrisiko / Begrenzt (Transparenz) / Minimal
FRIA-Referenz (Art 27)	Falls Hochrisiko und im Anwendungsbereich: Referenz der gemeinsamen Dokumentation