KOSTENLOS VON WECANDO.AI

Datenschutz-Folgenabschätzung (DSFA) für KI-Tools — Kurzformat für KMUs

Herausgeber: wecando.ai • Stand: April 2026 • Version: 1.0

wecando.ai – Die KI-Plattform für Macher
Stand: April 2026 | Version 1.0

Datenschutz-Folgenabschätzung (DSFA) für KI-Tools — Kurzformat für KMUs

Herausgeber: wecando.ai | **Stand:** April 2026 | **Version:** 1.0

> *Dieses Dokument ist kein Rechtsrat. Eine DSFA nach Art. 35 DSGVO kann eine rechtliche Verpflichtung sein. Vor der endgültigen Durchführung sollte der betriebliche Datenschutzbeauftragte eingebunden und ggf. ein Fachanwalt hinzugezogen werden.*

Wann brauchst du eine DSFA für KI-Tools?

Art. 35 DSGVO schreibt eine Datenschutz-Folgenabschätzung vor, wenn eine Datenverarbeitung "voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat".

DSFA ist in der Regel erforderlich bei:

- **Automatisierte Entscheidungsfindung** — KI trifft oder unterstützt Entscheidungen über Personen (Kreditwürdigkeit, Bewerbungsauswahl, Scoring)
- **Systematische Profilerstellung** — KI erstellt Profile von Kunden, Mitarbeitern oder Nutzern
- **Verarbeitung besonderer Datenkategorien** — Gesundheitsdaten, biometrische Daten, politische Meinungen in KI-Tools
- **Groß angelegte Verarbeitung** — KI verarbeitet Daten einer großen Anzahl Betroffener
- **Neue Technologien** — Erstmaliger Einsatz einer KI-Technologie im Unternehmen (die DSK-Positivliste nennt KI explizit)

DSFA ist in der Regel NICHT erforderlich bei:

- KI-Tools die nur generische Texte ohne Personenbezug erstellen
- Übersetzungstools für allgemeine Dokumente
- Bildgenerierung ohne Bezug zu realen Personen
- Interne Brainstorming-Nutzung ohne Dateneingabe

Schwellenwert-Check (Schnelltest)

Treffen **zwei oder mehr** der folgenden Kriterien zu, ist eine DSFA durchzuführen:

Nr.	Kriterium	Trifft zu?
1	Bewertung oder Scoring von Personen	☐

Nr.	Kriterium	Trifft zu?
2	Automatisierte Entscheidung mit rechtlicher Wirkung	☐
3	Systematische Überwachung	☐
4	Verarbeitung sensibler Daten (Art. 9 DSGVO)	☐
5	Verarbeitung in großem Umfang	☐
6	Abgleich oder Zusammenführung von Datensätzen	☐
7	Daten schutzbedürftiger Personen (Beschäftigte, Patienten)	☐
8	Innovative Nutzung neuer Technologien	☐
9	Betroffene können Recht/Dienstleistung nicht wahrnehmen ohne Verarbeitung	☐

Ergebnis: 0-1 Treffer = DSFA i.d.R. nicht nötig. 2+ Treffer = DSFA durchführen.

DSFA-Kurzformat: Template zum Ausfüllen

1. Allgemeine Angaben

Feld	Eintrag
Bezeichnung des KI-Tools	[Name des Tools, z.B. ChatGPT Enterprise]
Anbieter	[z.B. OpenAI, Inc.]
Version / Plan	[z.B. Enterprise, API, Pro]
Verantwortliche Stelle	[Firmenname, Anschrift]
Datenschutzbeauftragter	[Name, Kontakt]
Erstellt am	[Datum]
Erstellt von	[Name, Rolle]
Nächste Überprüfung	[Datum, spätestens 12 Monate]

2. Beschreibung des Verarbeitungsvorgangs

Zweck der Verarbeitung: [Wozu wird das KI-Tool eingesetzt? Welches Problem wird gelöst?]

Art der verarbeiteten Daten:

- ☐ Allgemeine personenbezogene Daten (Name, E-Mail, etc.)
- ☐ Beschäftigtendaten
- ☐ Kundendaten
- ☐ Besondere Datenkategorien (Gesundheit, Biometrie, etc.)
- ☐ Keine personenbezogenen Daten

Kategorien betroffener Personen:

- ☐ Kunden / Interessenten
- ☐ Beschäftigte
- ☐ Geschäftspartner / Lieferanten
- ☐ Sonstige: [angeben]

Anzahl Betroffener (geschätzt): [z.B. ca. 500 Kunden/Monat]

Datenfluss: [Woher kommen die Daten? → Wo werden sie eingegeben? → Wo werden sie verarbeitet? → Wo werden Ergebnisse gespeichert?]

---

3. Notwendigkeit und Verhältnismäßigkeit

Frage	Antwort
Ist der Einsatz des KI-Tools für den Zweck notwendig?	[Ja/Nein + Begründung]
Gibt es weniger eingriffsintensive Alternativen?	[Ja/Nein + welche?]
Werden nur die minimal notwendigen Daten verarbeitet (Datenminimierung)?	[Ja/Nein + Maßnahmen]
Ist die Speicherdauer begrenzt?	[Ja/Nein + Dauer]
Werden Betroffene informiert (Transparenz)?	[Ja/Nein + wie?]
Können Betroffene ihre Rechte ausüben (Auskunft, Löschung, Widerspruch)?	[Ja/Nein + Prozess]
Auf welcher Rechtsgrundlage basiert die Verarbeitung?	[Art. 6 Abs. 1 lit. a/b/c/f DSGVO]

---

4. Risikobewertung

Bewerte jedes Risiko nach: **Eintrittswahrscheinlichkeit (E)** x **Schwere (S)** = **Risikostufe (R)**

Skala: 1 = gering, 2 = niedrig, 3 = mittel, 4 = hoch, 5 = sehr hoch

Nr.	Risiko	E (1-5)	S (1-5)	R (ExS)	Stufe
R1	Unbefugter Zugriff auf eingegebene Daten				
R2	Daten werden für KI-Training genutzt (trotz Opt-out)				
R3	Datentransfer in unsicheres Drittland				
R4	Falsche KI-Ergebnisse führen zu fehlerhaften Entscheidungen				
R5	Versehentliche Eingabe sensibler Daten durch Beschäftigte				
R6	Mangelnde Löschbarkeit eingegebener Daten				
R7	Diskriminierende KI-Ergebnisse (Bias)				
R8	[Weiteres individuelles Risiko]				

Risikostufenmatrix:

Risikostufe (R)	Bewertung	Maßnahme
1–5	Geringes Risiko	Akzeptabel, Monitoring ausreichend
6–10	Mittleres Risiko	Maßnahmen erforderlich, Restrisiko dokumentieren

Risikostufe (R)	Bewertung	Maßnahme
11–15	Hohes Risiko	Zusätzliche Schutzmaßnahmen zwingend
16–25	Sehr hohes Risiko	Verarbeitung nur bei überzeugenden Maßnahmen, ggf. Aufsichtsbehörde konsultieren

5. Technisch-organisatorische Maßnahmen (TOMs)

Risiko-Nr.	Maßnahme	Verantwortlich	Umgesetzt?
R1	[z.B. Zugang nur über SSO, Berechtigungskonzept]	[Name]	☐
R2	[z.B. Training Opt-out aktiviert, vertraglich gesichert]	[Name]	☐
R3	[z.B. EU-Datenverarbeitung gewählt, SCCs abgeschlossen]	[Name]	☐
R4	[z.B. Vier-Augen-Prinzip, menschliche Überprüfung]	[Name]	☐
R5	[z.B. Schulung, Nutzungsrichtlinie, techn. Filter]	[Name]	☐
R6	[z.B. AVV mit Löschklausel, regelmäßige Prüfung]	[Name]	☐
R7	[z.B. Ergebnisse auf Bias prüfen, diverse Testdaten]	[Name]	☐

6. Ergebnis und Entscheidung

Gesamtbewertung	☐ Geringes Restrisiko — Verarbeitung zulässig
	☐ Mittleres Restrisiko — Verarbeitung unter Auflagen zulässig
	☐ Hohes Restrisiko — Zusätzliche Maßnahmen erforderlich vor Start

Gesamtbewertung	■ Geringes Restrisiko — Verarbeitung zulässig
	■ Sehr hohes Restrisiko — Konsultation der Aufsichtsbehörde (Art. 36 DSGVO)

Entscheidung: [Freigabe / Freigabe mit Auflagen / Ablehnung / Aufsichtsbehörde konsultieren]

Begründung: [Kurze Zusammenfassung der Abwägung]

Unterschriften:

	Datum	Unterschrift
Verantwortlicher	[DATUM]	_____
Datenschutzbeauftragter	[DATUM]	_____
[ggf. Betriebsrat]	[DATUM]	_____

Vorgefülltes Beispiel: ChatGPT im Kundensupport

Zur Orientierung ein ausgefülltes Beispiel. **Nicht 1:1 übernehmen** — deine Situation ist anders.

---

1. Allgemeine Angaben

Feld	Eintrag
Bezeichnung	ChatGPT Enterprise
Anbieter	OpenAI, Inc. (San Francisco, USA)
Version	Enterprise (via Microsoft Azure)
Verantwortliche Stelle	Muster GmbH, Musterstraße 1, 70000 Stuttgart
DSB	Maria Schmidt, dsb@muster-gmbh.de
Erstellt am	15.04.2026
Nächste Überprüfung	15.04.2027

2. Beschreibung

Zweck: Support-Mitarbeiter nutzen ChatGPT Enterprise um Antworten auf Kundenanfragen (E-Mail, Chat) zu formulieren. Die KI schlägt Antworten vor, Mitarbeiter prüfen und versenden sie.

Daten: Kundennamen, E-Mail-Adressen, Anfrageinhalte (teils Vertragsdaten, Bestellnummern). Keine besonderen Kategorien.

Betroffene: Ca. 2.000 Kunden/Monat, 15 Support-Mitarbeiter.

Datenfluss: Kundenanfrage (E-Mail/Chat) → Mitarbeiter kopiert Anfrage in ChatGPT (pseudonymisiert) → ChatGPT generiert Antwortvorschlag → Mitarbeiter prüft, ergänzt persönliche Anrede, versendet über CRM.

3. Verhältnismäßigkeit

- Notwendig? **Ja** — Antwortzeit soll von 24h auf 4h reduziert werden
- Alternativen? **Vorlagen-System** — weniger flexibel, deckt nur Standardfälle ab
- Datenminimierung? **Ja** — Kundennamen werden vor Eingabe durch "Kunde" ersetzt, Bestellnummern bleiben (kein Personenbezug)
- Rechtsgrundlage: **Art. 6 Abs. 1 lit. f DSGVO** (berechtigtes Interesse: effizienterer Kundenservice)

4. Risikobewertung

Nr.	Risiko	E	S	R	Stufe
R1	Unbefugter Zugriff	2	3	6	Mittel
R2	Training auf Daten	1	4	4	Gering
R3	Datentransfer USA	2	3	6	Mittel
R4	Falsche Antworten	3	2	6	Mittel
R5	Versehentlich Klarnamen eingegeben	3	3	9	Mittel

5. Maßnahmen

Risiko	Maßnahme
R1	SSO-Login, nur Support-Team hat Zugang, vierteljährlicher Access Review
R2	Enterprise-Plan: kein Training. Vertraglich im DPA gesichert

Risiko	Maßnahme
R3	EU Data Boundary bei Azure aktiviert, SCCs im DPA
R4	Vier-Augen-Prinzip: Jede KI-Antwort wird vor Versand geprüft
R5	Schulung (vierteljährlich), Pseudonymisierungs-Checkliste am Arbeitsplatz, stichprobenartige Prüfung

6. Ergebnis

Gesamtbewertung: Mittleres Restrisiko — Verarbeitung unter Auflagen zulässig.

Auflagen: Pseudonymisierungspflicht, vierteljährliche Schulung, halbjährliche DSFA-Überprüfung, Logging der ChatGPT-Nutzung (aggregiert, nicht personenbezogen).

Weiterführende Quellen

- **DSK-Kurzpapier Nr. 5:** Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
- **DSK-Positivliste:** Verarbeitungstätigkeiten die eine DSFA erfordern (enthält KI-basierte Verarbeitungen)
- **Art. 35–36 DSGVO:** Rechtsgrundlage DSFA + Konsultation Aufsichtsbehörde
- **Mehr Praxiswissen:** wecando.ai/ki-business

Erstellt von wecando.ai — Die KI-Plattform für Macher. Stand: April 2026. Dieses Dokument ist kein Rechtsrat. Vor verbindlicher Verwendung Fachanwalt konsultieren.

Naechste Schritte

1	Mache den Schwellenwert-Check auf Seite 1 fuer dein wichtigstes KI-Tool
2	Falls 2+ Treffer: Fuell das DSFA-Template mit deinem Datenschutzbeauftragten aus
3	Dokumentiere das Ergebnis und plane die naechste Ueberpruefung in 12 Monaten

Mehr kostenlose Ressourcen

Alle Lead Magnets sind kostenlos. Keine Anmeldung noetig.

- [ ] **DSGVO-KI-Compliance-Paket**
  4 Vorlagen: Checkliste, BV, Datenschutzhinweis, DSFA
  wecando.ai/ki-business/dsgvo-ki-compliance-paket/

- [ ] **30 Prompt-SYSTEME**
  Copy-Paste Workflows fuer ChatGPT, Claude & Co.
  wecando.ai/ki-wissen/prompt-systeme-workflows/

- [ ] **KI-Blacklist: 23 Fehler**
  Die haeufigsten KI-Fehler und wie du sie vermeidest
  wecando.ai/ki-wissen/ki-blacklist/

- [ ] **150 Prompts Swipe-File**
  Sofort einsetzbare Prompts fuer jede Situation
  wecando.ai/ki-wissen/ki-prompt-swipe-file/

- [ ] **KI-Toolstack (7 Branchen)**
  Branchenspezifische Tool-Empfehlungen mit Preisen
  wecando.ai/ki-business/ki-toolstack-branchen/

- [ ] **KI in 7 Tagen (Kurs)**
  Vom Anfaenger zum KI-Anwender in einer Woche
  wecando.ai/ki-wissen/ki-in-7-tagen-kurs/

- [ ] **KI-ROI-Rechner**
  Berechne deine KI-Ersparnis in 2 Minuten
  wecando.ai/ki-tools/ki-roi-rechner/

wecando.ai – Die groesste deutschsprachige KI-Informationssammlung