DATENSCHUTZ-FOLGENABSCHÄTZUNG

KI-SCHNELLCHECK FÜR KMU

DSFA-Light für KI

Template – Schnellcheck für KMU

In **20–30 Minuten** erkennen, ob eine Datenschutz-Folgenabschätzung wahrscheinlich nötig ist.

Dieses praxisnahe Template führt Sie Schritt für Schritt durch eine strukturierte Vorprüfung Ihrer KI-Projekte. Von der Use-Case-Beschreibung über die Risikobewertung bis zur dokumentierten Entscheidung – alles in einem kompakten, ausfüllbaren Format. Entwickelt für Datenschutzverantwortliche, KI-Projektleiter und Geschäftsführer kleiner und mittlerer Unternehmen, die KI-Tools rechtskonform einsetzen wollen, ohne sich in bürokratischen Prozessen zu verlieren.

Ziel & Definition of Done

Bevor Sie mit der Vorprüfung beginnen, sollten Sie genau wissen, **was dieses Template leisten soll** und **wann Sie fertig sind**. Die folgenden Abschnitte definieren beides klar und verbindlich. So stellen Sie sicher, dass Ihre DSFA-Light nicht nur begonnen, sondern vollständig und dokumentiert abgeschlossen wird – ein entscheidender Faktor für die Nachweispflicht gegenüber Aufsichtsbehörden.

🎯 Ziel dieses Templates

Dieses Template dient zwei klar definierten Zwecken, die jedes KI-Projekt vor dem Go-Live durchlaufen sollte:

Schnelle Vorprüfung

Eine schnelle, dokumentierte Vorprüfung zu Datenschutzrisiken durchführen – strukturiert, nachvollziehbar und auditfähig. Sie erhalten in wenigen Minuten Klarheit darüber, ob Ihr KI-Einsatz datenschutzrechtlich kritisch ist.

Konkreter Maßnahmenplan

Einen konkreten Maßnahmenplan erstellen, bevor Sie live gehen. Damit vermeiden Sie nachträgliche Korrekturen, die erfahrungsgemäß deutlich teurer und aufwändiger sind als eine vorausschauende Planung.

✅ Definition of Done

Ihre DSFA-Light ist abgeschlossen, wenn alle vier Kriterien erfüllt sind. Erst dann gilt die Vorprüfung als vollständig dokumentiert und belastbar:

01

Daten & Zweck beschrieben

Welche Daten werden wofür verarbeitet? Welches KI-System kommt zum Einsatz? Alles ist klar benannt und nachvollziehbar.

02

Risiko grob bewertet

Eintrittswahrscheinlichkeit und Schadensausmaß sind eingeschätzt. Die Risiko-Matrix ist ausgefüllt.

03

Entscheidung dokumentiert

DSFA ja oder nein – mit nachvollziehbarer Begründung. Diese Dokumentation ist Ihr Nachweis gegenüber Behörden.

04

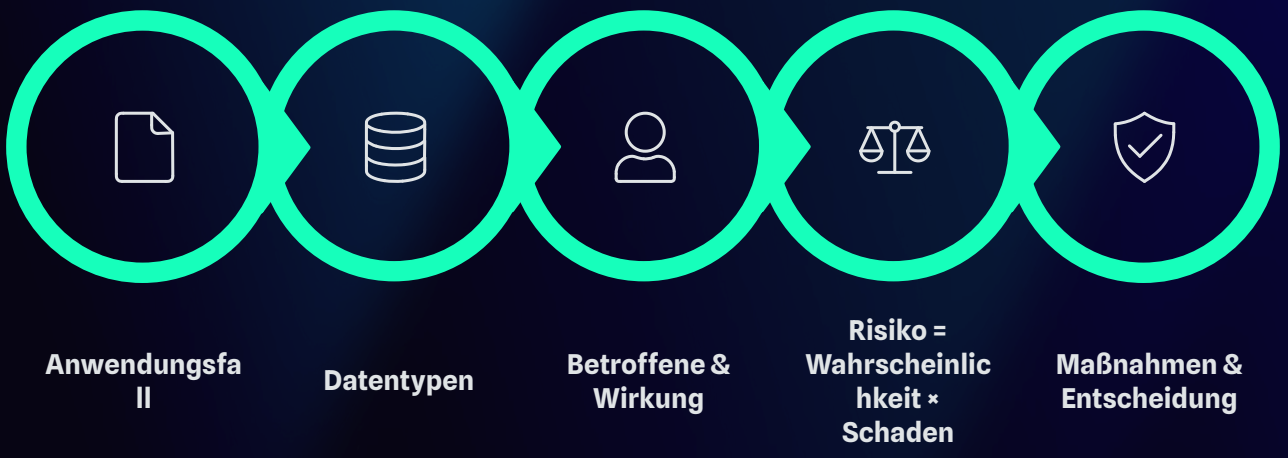
Maßnahmen & Owner gesetzt

Jede identifizierte Maßnahme hat einen Verantwortlichen und einen Termin. Nichts bleibt unverbindlich.

Wichtig: Dieses Template ersetzt keine vollständige DSFA nach Art. 35 DSGVO. Es dient als strukturierte Vorprüfung, um festzustellen, ob eine umfassende DSFA notwendig ist. Dokumentieren Sie immer – auch wenn das Ergebnis „keine DSFA nötig" lautet.

DSFA-Light Flow – 5 Schritte zum Ergebnis

Der gesamte Schnellcheck folgt einem klaren, linearen Ablauf aus fünf Schritten. Jeder Schritt baut auf dem vorherigen auf und führt Sie systematisch von der Beschreibung Ihres KI-Anwendungsfalls bis zur finalen, dokumentierten Entscheidung. Planen Sie insgesamt **20 bis 30 Minuten** ein – idealerweise gemeinsam mit dem fachlich Verantwortlichen für das KI-Projekt.



Dieser Flow ist so konzipiert, dass er auch ohne tiefgehende juristische Kenntnisse durchlaufen werden kann. Die einzelnen Templates auf den folgenden Seiten liefern Ihnen für jeden Schritt die passende Struktur mit konkreten Feldern, Checkboxen und Bewertungshilfen. Wichtig ist, dass Sie **jeden Schritt vollständig ausfüllen**, bevor Sie zum nächsten übergehen. Unvollständige Angaben führen zu einer unbrauchbaren Dokumentation.

Schritt 1–2

Fakten sammeln: Was wird gemacht, welche Daten fließen?

Schritt 3–4

Risiko bewerten: Wer ist betroffen, wie hoch ist das Risiko?

Schritt 5

Entscheiden & handeln: Maßnahmen festlegen, Ergebnis dokumentieren.

Template 1: Use-Case Steckbrief

SCHRITT 1 VON 5 FORMULAR ZUM AUSFÜLLEN

Beginnen Sie mit einer klaren Beschreibung Ihres KI-Anwendungsfalls. Dieser Steckbrief bildet die Grundlage für alle weiteren Bewertungen. Nehmen Sie sich ausreichend Zeit, um die Felder präzise auszufüllen – je genauer Ihre Angaben hier sind, desto belastbarer wird Ihre gesamte Vorprüfung. Füllen Sie den Steckbrief gemeinsam mit dem Projektverantwortlichen aus, um sicherzustellen, dass keine relevanten Aspekte übersehen werden.

Use-Case Name	_____
System / Tool	_____
Zweck (1–2 Sätze)	_____
Output / Entscheidung	_____
Nutzergruppe (intern)	_____
Betroffene	_____
Go-Live Datum	_____
Owner	_____

💡 **Tipp – Zweck:** Beschreiben Sie den Zweck so konkret wie möglich. Statt „Kundenservice verbessern" besser: „Automatische Kategorisierung eingehender Support-Tickets nach Dringlichkeit und Thema mittels GPT-4, um Bearbeitungszeit um 40 % zu senken."

💡 **Tipp – Betroffene:** Denken Sie breit: Kund:innen, Mitarbeitende, Bewerber:innen, Lieferanten, Partner. Auch indirekt Betroffene zählen – z. B. Personen, deren Daten in Trainingsdaten enthalten sein könnten.

Der Use-Case Steckbrief sollte für **jedes einzelne KI-Projekt** separat ausgefüllt werden. Wenn Sie mehrere Tools einsetzen, die unterschiedliche Daten verarbeiten oder unterschiedliche Zwecke verfolgen, erstellen Sie jeweils einen eigenen Steckbrief. Dies erleichtert später auch die Zuordnung von Maßnahmen und Verantwortlichkeiten erheblich.

Template 2: Daten & Verarbeitung

SCHRITT 2 VON 5 | FORMULAR ZUM AUSFÜLLEN

Im zweiten Schritt erfassen Sie systematisch, **welche Datenarten** in Ihrem KI-Projekt verarbeitet werden, **woher diese Daten stammen** und **wo sie gespeichert werden**. Diese Informationen sind entscheidend für die spätere Risikobewertung. Besondere Aufmerksamkeit verdienen sogenannte besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sowie die Frage, ob der KI-Anbieter selbst Zugriff auf die Daten hat.

Datenarten – bitte ankreuzen

☐ Name
Vor- und Nachname von Betroffenen

☐ E-Mail
E-Mail-Adressen geschäftlich/privat

☐ Telefonnr.
Festnetz- oder Mobilnummern

☐ Kaufdaten
Bestellhistorie, Warenkörbe, Zahlungen

☐ Standort
GPS, IP-basiert, Adressdaten

☐ Tickettexte
Support-Anfragen, Freitexte

☐ Sensor-/Maschinendaten
IoT-Daten, Maschinenlogs

☐ Sonstiges
_____

Weitere Angaben zur Verarbeitung

Besondere Kategorien? (Art. 9 DSGVO)	☐ Ja → _____ ☐ Nein
Datenquelle	☐ CRM ☐ ERP ☐ Shop ☐ Tickets ☐ Manuell ☐ Sensoren
Speicherung / Region	☐ EU ☐ Non-EU ☐ Unbekannt
Inputs/Prompts beim Anbieter gespeichert?	☐ Ja ☐ Nein ☐ Unbekannt
Training durch Anbieter?	☐ Ja ☐ Nein ☐ Unbekannt

⚠️ **Achtung:** Wenn Inputs/Prompts beim Anbieter gespeichert werden oder für Training genutzt werden, steigt das Risiko erheblich. Prüfen Sie die AGB und DPA (Data Processing Agreement) des Anbieters sorgfältig. Bei „Unbekannt" empfiehlt sich eine direkte Nachfrage beim Anbieter – dokumentieren Sie die Antwort.

Template 3: Risiko-Fragen

⚠ SCHRITT 3 VON 5 | JA / NEIN + KOMMENTAR

Die folgenden zehn Fragen orientieren sich an den Kriterien der Datenschutz-Aufsichtsbehörden und der Art.-29-Datenschutzgruppe zur Bestimmung, ob eine DSFA erforderlich ist. Als **Faustregel** gilt: Werden **zwei oder mehr Fragen mit „Ja" beantwortet**, ist eine vollständige DSFA nach Art. 35 DSGVO mit hoher Wahrscheinlichkeit notwendig. Beantworten Sie jede Frage ehrlich und ergänzen Sie in der Kommentarspalte relevante Kontextinformationen.

Nr.	Frage	Ja/Nein	Kommentar
1	Profiling/Scoring von Personen?	☐ J ☐ N	_____
2	Automatisierte Entscheidungen mit Wirkung auf Personen?	☐ J ☐ N	_____
3	Verarbeitung großer Mengen personenbezogener Daten?	☐ J ☐ N	_____
4	Überwachung von Mitarbeitenden?	☐ J ☐ N	_____
5	Drittlandtransfer wahrscheinlich?	☐ J ☐ N	_____
6	Sensitive/abgeleitete Daten (z. B. Verhalten/Emotion)?	☐ J ☐ N	_____
7	Hohe Erwartung an Vertraulichkeit (Supportfälle)?	☐ J ☐ N	_____
8	Keine klare Rechtsgrundlage vorhanden?	☐ J ☐ N	_____
9	Datenminimierung nicht möglich?	☐ J ☐ N	_____
10	Transparenz gegenüber Betroffenen unklar?	☐ J ☐ N	_____

⩾2×

Ja-Antworten

Ab zwei „Ja"-Antworten ist eine vollständige DSFA sehr wahrscheinlich erforderlich.

1×

Ja-Antwort

Bei einer „Ja"-Antwort: Genau prüfen und gut begründen, warum keine DSFA nötig ist.

0×

Ja-Antworten

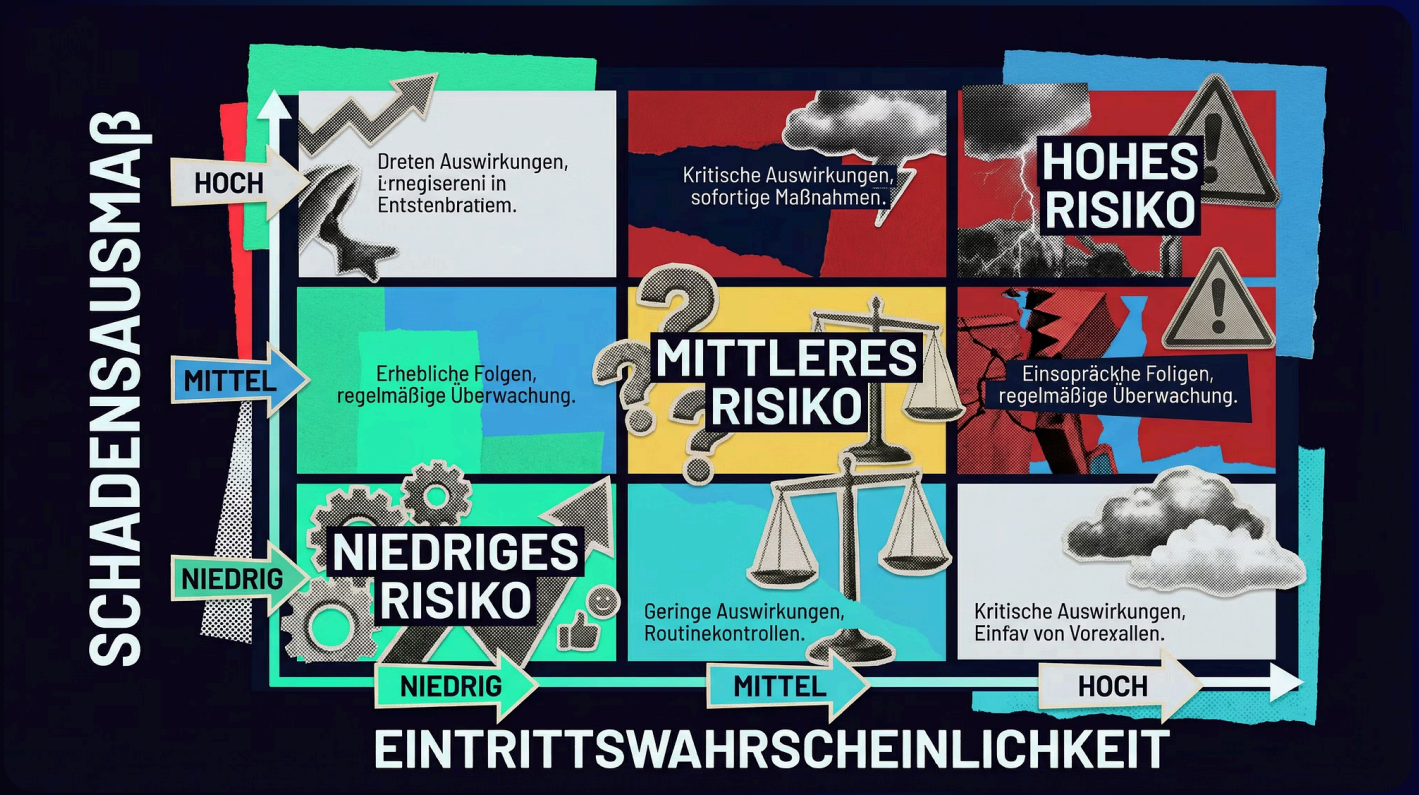
Kein „Ja": DSFA voraussichtlich nicht erforderlich. Dokumentation trotzdem aufbewahren.

Zählen Sie Ihre „Ja"-Antworten und tragen Sie die Gesamtzahl hier ein: **Anzahl „Ja": ____**

Template 4: Risiko-Matrix

SCHRITT 4 VON 5 | EINTRITT × SCHADEN

Die Risiko-Matrix kombiniert zwei Dimensionen: die **Eintrittswahrscheinlichkeit** (wie wahrscheinlich ist es, dass das Risiko eintritt?) und das **Schadensausmaß** (wie schwer wären die Folgen für die betroffenen Personen?). Diese klassische Methode wird von Aufsichtsbehörden empfohlen und liefert eine nachvollziehbare, visuelle Bewertungsgrundlage für Ihre Entscheidung.



Ihre Bewertung

Eintrittswahrscheinlichkeit	☐ Niedrig ☐ Mittel ☐ Hoch
Schadensausmaß	☐ Niedrig ☐ Mittel ☐ Hoch
Gesamtrisiko (Ampel)	🟢 Grün 🟡 Gelb 🔴 Rot

Begründung

_____

_____

_____

🟢 Grün – Niedriges Risiko

Dokumentation aufbewahren, Regelbetrieb möglich. Keine DSFA notwendig.

🟡 Gelb – Mittleres Risiko

Maßnahmen definieren, ggf. Rücksprache mit DSB. DSFA prüfen.

🔴 Rot – Hohes Risiko

DSFA durchführen. Vor Go-Live zwingend Maßnahmen umsetzen.

Template 5: Maßnahmenplan & Entscheidung

SCHRITT 5 VON 5 | FINALE DOKUMENTATION

Im letzten Schritt überführen Sie alle identifizierten Risiken in **konkrete, terminierte Maßnahmen** und dokumentieren Ihre Entscheidung. Dieser Abschnitt ist das Herzstück Ihrer Dokumentation – er zeigt Aufsichtsbehörden, dass Sie Risiken nicht nur erkannt, sondern aktiv gemanagt haben. Jede Maßnahme braucht einen Owner und einen verbindlichen Termin. Ohne klare Verantwortlichkeiten bleiben Maßnahmen wirkungslos.

Maßnahmenplan

Risiko / Problem	Maßnahme (TOM/Prozess)	Owner	Termin	Status
_____	_____	_____	_____	☐ Offen
_____	_____	_____	_____	☐ Offen
_____	_____	_____	_____	☐ Offen
_____	_____	_____	_____	☐ Offen
_____	_____	_____	_____	☐ Offen

Entscheidungsbox

Entscheidung: DSFA erforderlich?

☐ **Ja** – Vollständige DSFA nach Art. 35 DSGVO wird durchgeführt.

☐ **Nein** – Keine DSFA erforderlich. Begründung liegt vor.

Begründung (max. 4 Zeilen)

_____
_____
_____
_____
_____
_____
_____
_____

Review-Datum

Nächste Überprüfung am:
____.____.________

Verantwortlich:
_____

📌 **Hinweis:** Planen Sie einen regelmäßigen Review-Zyklus ein (z. B. alle 6 Monate oder bei wesentlichen Änderungen am KI-System). Änderungen an Datenquellen, Zwecken oder Anbieter-AGBs können eine Neubewertung erfordern. Bewahren Sie dieses ausgefüllte Template **mindestens 3 Jahre** auf.

Zusammenfassung & Schnellreferenz

Sie haben alle fünf Templates durchgearbeitet? Nutzen Sie diese Übersicht als Schnellreferenz, um sicherzustellen, dass Ihre DSFA-Light vollständig ist. Haken Sie jeden Punkt ab und stellen Sie sicher, dass keine Lücken in Ihrer Dokumentation verbleiben. Diese Checkliste eignet sich auch hervorragend als Deckblatt für Ihre abgeheftete oder digital archivierte Vorprüfung.

1

Use-Case Steckbrief

- ☐ Alle 8 Felder vollständig ausgefüllt
- ☐ Zweck präzise formuliert
- ☐ Betroffene identifiziert

2

Daten & Verarbeitung

- ☐ Datenarten angekreuzt
- ☐ Speicherregion geklärt
- ☐ Anbieter-Speicherung geprüft

3

Risiko-Fragen

- ☐ Alle 10 Fragen beantwortet
- ☐ Kommentare ergänzt
- ☐ Ja-Antworten gezählt

4

Risiko-Matrix

- ☐ Eintritt × Schaden bewertet
- ☐ Ampelfarbe bestimmt
- ☐ Begründung formuliert

5

Maßnahmen & Entscheidung

- ☐ Alle Maßnahmen mit Owner
- ☐ DSFA-Entscheidung getroffen
- ☐ Review-Datum gesetzt

> **Tipp:** Drucken Sie dieses Template aus oder speichern Sie es als PDF. Füllen Sie es für jedes neue KI-Projekt separat aus. Bei Änderungen am bestehenden Projekt – neue Datenquellen, neuer Anbieter, geänderter Zweck – durchlaufen Sie den Flow erneut.

Ressourcen & Kontakt

Sie haben die DSFA-Light abgeschlossen – oder möchten sich weiter in das Thema KI und Datenschutz vertiefen? Hier finden Sie weiterführende Ressourcen, das passende Buch zum Thema und den direkten Kontakt für Rückfragen. Nutzen Sie den QR-Code, um die digitale Version dieses Templates sowie zusätzliche Materialien herunterzuladen.

Weiterführende Ressourcen

- **Art. 35 DSGVO**

  Offizielle Rechtsgrundlage zur Datenschutz-Folgenabschätzung – die gesetzliche Basis für dieses Template.

- **DSK Muss-Liste**

  Liste der Verarbeitungstätigkeiten, für die eine DSFA zwingend durchzuführen ist (Datenschutzkonferenz).

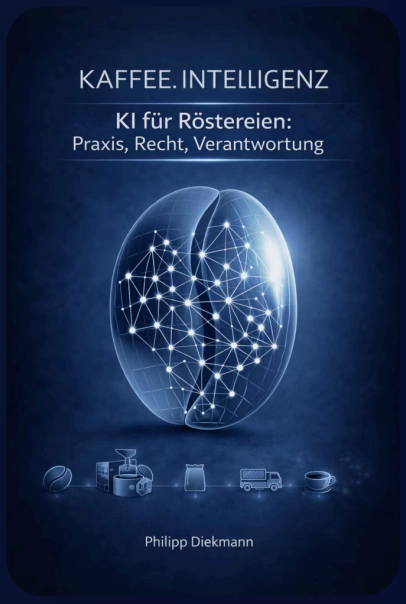
- **EDSA Leitlinien zur KI**

  Europäischer Datenschutzausschuss: aktuelle Empfehlungen zum Einsatz von KI-Systemen und Datenschutz.

- **BSI Grundschutz KI**

  Technische Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zu KI-Absicherung.

📖 Buchtipp



KI-Kompass für KMU – Das Praxisbuch für den sicheren Einstieg in künstliche Intelligenz. Von der Strategie über den Datenschutz bis zum produktiven Einsatz: Alles, was kleine und mittlere Unternehmen wissen müssen.

Jetzt entdecken auf kaffee-intelligenz.de

Website
kaffee-intelligenz.de

E-Mail
philipp@kaffee-intelligenz.de

Kontakt
Philipp Diekmann