

Playbook

AI Act Risiko-Matrix

Use Cases einordnen, Pflichten erkennen, nächste Schritte ableiten

Ein praxisorientierter Leitfaden für kleine und mittlere Unternehmen, die ihre KI-Anwendungen rechtskonform und strukturiert bewerten möchten – entwickelt von **Philipp Diekmann** | kaffee-intelligenz.de



Risiko

Klassen
verstehen



Einstufen

Use Cases
bewerten



Pflichten

Maßnahmen
ableiten



Umsetzen

Dokumentiert
handeln

Ziel & Definition of Done

Dieses Playbook gibt Ihnen einen klaren, strukturierten Rahmen an die Hand, um Ihre KI-Anwendungen nach den Vorgaben des EU AI Acts einzuordnen und die daraus resultierenden Pflichten systematisch abzuleiten. Es richtet sich an Entscheider:innen und Verantwortliche in KMU, die pragmatisch und ohne juristischen Overhead handlungsfähig werden möchten. Die folgenden Ziele definieren, was Sie nach dem Durcharbeiten dieses Playbooks erreicht haben werden.

Ziele dieses Playbooks

1 Risikoklassen einordnen

Du ordnest deine KI-Use-Cases systematisch in die **4 Risikoklassen** des AI Acts ein – von minimal bis unverträglich.

2 Pflichten ableiten

Du leitest **pragmatische Pflichten und konkrete ToDos** je Risikoklasse ab, ohne dich in juristischen Details zu verlieren.

3 Entscheidung dokumentieren

Du dokumentierst jede Einstufung mit **Owner und Review-Datum**, damit Compliance nachvollziehbar bleibt.

Definition of Done

Ihr Playbook-Durchlauf ist abgeschlossen, wenn folgende drei Kriterien erfüllt sind:

1 • Klassifiziert


Jeder Use Case ist einer Risikoklasse zugeordnet

2 • Pflichtenliste

Pro Use Case existiert eine konkrete Pflichtenliste

3 • Owner gesetzt

Verantwortliche:r und Review-Datum sind dokumentiert

 **Disclaimer:** Dieses Playbook dient der **Orientierung** und ersetzt keine individuelle Rechtsberatung. Bei konkreten rechtlichen Fragestellungen wenden Sie sich bitte an eine qualifizierte Rechtsberatung. Weitere Informationen finden Sie auf www.kaffee-intelligenz.de.

Die Risikolandkarte des AI Acts

Der EU AI Act teilt KI-Systeme in vier Risikoklassen ein. Diese Klassifikation ist das Fundament Ihrer gesamten Compliance-Strategie. Je höher die Risikoklasse, desto strenger die regulatorischen Anforderungen. Die folgende Matrix zeigt Ihnen auf einen Blick, welche Klassen existieren und was sie für Ihr Unternehmen bedeuten. Entscheidend ist nicht das Tool selbst, sondern der **konkrete Use Case** – ein und dasselbe System kann je nach Einsatzzweck unterschiedlich eingestuft werden.



Die Einordnung in diese vier Klassen ist der erste und wichtigste Schritt Ihrer AI-Act-Compliance. Für KMU im Bereich Kaffee und Lebensmittel ergeben sich typische Anwendungsfälle in jeder Kategorie: Von harmlosen Textvorschlägen für Produktbeschreibungen über Chatbots für den Kundenservice bis hin zu sicherheitskritischen Qualitätssicherungsanalysen. Besonders aufmerksam sollten Sie bei HR-Anwendungen und qualitätsentscheidenden Systemen sein – diese fallen häufig in die Kategorie **Hoch** und unterliegen damit umfangreichen Pflichten.


Merke: Nicht das Tool bestimmt die Risikoklasse, sondern der **konkrete Einsatzzweck** in Ihrem Unternehmen.

Entscheidungsbaum: 5 Fragen zur Risikoklasse

Die Einstufung eines KI-Use-Cases muss nicht kompliziert sein. Mit nur fünf systematischen Fragen können Sie jeden Anwendungsfall in die richtige Risikoklasse einordnen. Arbeiten Sie den folgenden Entscheidungsbaum von oben nach unten durch – bei der ersten zutreffenden Antwort erhalten Sie Ihre vorläufige Klassifikation. Dieser pragmatische Ansatz eignet sich besonders für KMU, die schnell und strukturiert eine Ersteinschätzung vornehmen möchten.



Beachten Sie, dass dieser Entscheidungsbaum eine **Ersteinschätzung** liefert. In Grenzfällen – etwa wenn ein System sowohl interne Prozesse steuert als auch kundenseitig eingesetzt wird – sollten Sie den konservativeren Pfad wählen und die höhere Risikoklasse ansetzen. Die finale Bewertung sollte stets im Kontext des spezifischen Einsatzszenarios und unter Berücksichtigung der betroffenen Personen erfolgen. Dokumentieren Sie Ihre Entscheidungslogik nachvollziehbar in der Risiko-Matrix auf den folgenden Seiten.

 **Tipp:** Durchlaufen Sie den Entscheidungsbaum für jeden Use Case separat – nicht für das gesamte Tool. Ein CRM-System kann gleichzeitig minimale und begrenzte Risikoanwendungen beinhalten. Mehr Praxisbeispiele finden Sie auf www.kaffee-intelligenz.de.

Pflichten-Überblick: Hochrisiko-KI

⚠ RISIKOKLASSE HOCH

Wenn Ihr KI-System als **Hochrisiko** eingestuft wurde, gelten die strengsten Anforderungen des AI Acts. Diese sieben zentralen Pflichten bilden das Kerngerüst Ihrer Compliance-Maßnahmen. Sie sind darauf ausgelegt, Risiken systematisch zu identifizieren, zu minimieren und transparent zu dokumentieren. Für KMU mag dieser Katalog zunächst umfangreich erscheinen – doch mit einer strukturierten Herangehensweise lassen sich die Anforderungen pragmatisch und schrittweise umsetzen.

1

Risikomanagementsystem

Etablieren Sie ein systematisches Verfahren zur Identifikation, Bewertung und Minderung von Risiken über den gesamten Lebenszyklus des KI-Systems.

2

Daten- & Qualitätsmanagement

Stellen Sie sicher, dass Trainings- und Testdaten relevant, repräsentativ, fehlerfrei und vollständig sind. Dokumentieren Sie Datenquellen und -verarbeitung.

3

Technische Dokumentation

Erstellen Sie umfassende technische Dokumentation **vor** dem Inverkehrbringen – inklusive Systemarchitektur, Trainingsprozess und Leistungskennzahlen.

4

Protokollierung & Nachvollziehbarkeit

Implementieren Sie automatische Protokollierung (Logging), um Entscheidungen und Systemverhalten nachvollziehbar zu machen und auditieren zu können.

5

Transparenz & Information

Informieren Sie Betroffene verständlich über den Einsatz des KI-Systems, seine Funktionsweise und die Auswirkungen auf sie.

6

Menschliche Aufsicht

Gewährleisten Sie, dass qualifizierte Personen das System überwachen, Ergebnisse prüfen und bei Bedarf eingreifen können.

7

Robustheit, Genauigkeit & Cybersicherheit

Sorgen Sie für ein angemessenes Maß an Genauigkeit, Robustheit gegen Fehler und Schutz vor Manipulation und Cyberangriffen.

Jede dieser Pflichten erfordert eine dokumentierte Umsetzung. Nutzen Sie die Risiko-Matrix-Vorlage auf der nächsten Seite, um pro Use Case die relevanten Pflichten zuzuordnen und Verantwortlichkeiten festzulegen. Detaillierte Umsetzungshilfen und Templates stehen auf www.kaffee-intelligenz.de zum Download bereit.

Risiko-Matrix Template

Die folgende Tabelle ist Ihr zentrales Arbeitsinstrument zur Dokumentation aller KI-Use-Cases in Ihrem Unternehmen. Füllen Sie sie für jedes KI-System bzw. jeden Use Case separat aus. Die Matrix dient als Nachweis Ihrer systematischen Auseinandersetzung mit dem AI Act und bildet die Grundlage für interne Audits, Datenschutzfolgenabschätzungen und Behördenanfragen. Drucken Sie diese Seite aus oder nutzen Sie die digitale Vorlage auf www.kaffee-intelligenz.de.

Use Case #1	Use Case #2	Use Case #3
Use Case: -----	Use Case: -----	Use Case: -----
System / Tool: -----	System / Tool: -----	System / Tool: -----
Betroffene: <input type="checkbox"/> Kund:innen <input type="checkbox"/> Mitarbeitende <input type="checkbox"/> Partner	Betroffene: <input type="checkbox"/> Kund:innen <input type="checkbox"/> Mitarbeitende <input type="checkbox"/> Partner	Betroffene: <input type="checkbox"/> Kund:innen <input type="checkbox"/> Mitarbeitende <input type="checkbox"/> Partner
Datenarten: -----	Datenarten: -----	Datenarten: -----
Risikoklasse: <input type="checkbox"/> Minimal <input type="checkbox"/> <input type="checkbox"/> Begrenzt <input type="checkbox"/> Hoch <input type="checkbox"/> <input type="checkbox"/> Unvertretbar	Risikoklasse: <input type="checkbox"/> Minimal <input type="checkbox"/> <input type="checkbox"/> Begrenzt <input type="checkbox"/> Hoch <input type="checkbox"/> <input type="checkbox"/> Unvertretbar	Risikoklasse: <input type="checkbox"/> Minimal <input type="checkbox"/> <input type="checkbox"/> Begrenzt <input type="checkbox"/> Hoch <input type="checkbox"/> <input type="checkbox"/> Unvertretbar
Pflichten / ToDos: -----	Pflichten / ToDos: -----	Pflichten / ToDos: -----
Owner: -----	Owner: -----	Owner: -----
Review-Datum: -----	Review-Datum: -----	Review-Datum: -----

Hinweise zum Ausfüllen

- **Use Case:** Beschreiben Sie den konkreten Einsatzzweck, nicht nur den Tool-Namen
- **Betroffene:** Wer ist von der KI-Entscheidung betroffen oder wird mit ihr konfrontiert?
- **Datenarten:** Welche Daten verarbeitet das System (personenbezogen, anonym, Sensordaten)?

Prozess-Empfehlung

- **Risikoklasse:** Nutzen Sie den Entscheidungsbaum von Seite 4
- **Pflichten:** Leiten Sie ab aus dem Pflichtenkatalog Seite 5
- **Owner:** Benennen Sie eine verantwortliche Person mit Entscheidungskompetenz
- **Review:** Setzen Sie ein Datum innerhalb von max. 12 Monaten

Praxisbeispiele: 3 ausgefüllte Use Cases

BRANCHENBEISPIELE KAFFEE & LEBENSMITTEL

Die Theorie wird greifbar, wenn Sie sie an konkreten Beispielen durchspielen. Die folgenden drei Use Cases zeigen, wie die Risiko-Matrix in der Praxis ausgefüllt wird. Diese Szenarien stammen aus typischen KMU-Kontexten der Kaffee- und Lebensmittelbranche und veranschaulichen die Bandbreite der Einstufungen von **Begrenzt** bis **Hoch**. Nutzen Sie diese als Orientierung für Ihre eigene Bewertung.

Chatbot Support

System: ChatGPT API / Custom Bot

Betroffene: Kund:innen

Datenarten: Anfragen, Kontaktdaten, Chat-Verläufe

Risikoklasse: **Begrenzt**

Pflichten/ToDos: Transparenzhinweis, Eskalation zu Mensch, Logging einrichten

Owner: Team Lead CS

Review: Q1/2026

Bewerber-Vorscreening

System: HR-Software mit KI-Scoring

Betroffene: Mitarbeitende / Bewerber:innen

Datenarten: Lebensläufe, Bewertungsscores, personenbezogene Daten

Risikoklasse: **Hoch**

Pflichten/ToDos: DSFA durchführen, menschliche Aufsicht, Dokumentation, Monitoring etablieren

Owner: HR-Leitung

Review: Q4/2025

QS Bild-/Sensoranalyse

System: Vision AI / Sensorplattform

Betroffene: Kund:innen (indirekt), Mitarbeitende

Datenarten: Produktbilder, Sensordaten, Qualitätsmetriken

Risikoklasse: **Hoch** (wenn qualitätsentscheidend)

Pflichten/ToDos: Testdatenset validieren, Doku erstellen, Freigabeprozess, Audit-Rhythmus festlegen

Owner: QS-Leitung

Review: Q2/2026

Chatbot Support

Ein KI-gestützter Chatbot auf der Website beantwortet Kundenfragen zu Produkten, Bestellungen und Lieferzeiten. Da er **direkt mit Kund:innen interagiert**, greift die Transparenzpflicht: Nutzer:innen müssen wissen, dass sie mit einer KI sprechen, und es muss jederzeit eine Eskalation zu einem Menschen möglich sein.

Bewerber-Vorscreening

Eine HR-Software bewertet eingehende Bewerbungen automatisch vor und erstellt ein Ranking. Da dieses System **direkte Auswirkungen auf den Zugang zu Beschäftigung** hat, ist es als Hochrisiko einzustufen. Die strengsten Pflichten des AI Acts greifen – inklusive Datenschutzfolgenabschätzung.

QS Bild-/Sensoranalyse

Ein Vision-AI-System prüft Kaffeebohnen oder Röstergebnisse automatisch auf Qualitätsmängel. Wenn dieses System **qualitätsentscheidend** ist und fehlerhafte Produkte durchlässt, hat dies direkte Auswirkungen auf Verbrauchersicherheit – daher Einstufung als Hoch.

Quick-Check & Typische Fehler

In der Praxis sehen wir immer wieder dieselben Fehler bei der AI-Act-Einstufung. Gerade KMU ohne dedizierte Compliance-Abteilung tapen in vermeidbare Fallen, die im Ernstfall zu empfindlichen Bußgeldern führen können. Der EU AI Act sieht Strafen von bis zu **35 Millionen Euro** oder **7 % des weltweiten Jahresumsatzes** vor – selbst für KMU ein existenzbedrohendes Risiko. Die folgende Übersicht zeigt die fünf häufigsten Fehler und gibt Ihnen einen Quick-Check zur sofortigen Selbstüberprüfung an die Hand.

🚫 Die 5 typischen Fehler

1 Nur Tool-Name dokumentiert

Statt den konkreten Use Case zu beschreiben, steht nur „ChatGPT“ oder „HubSpot“ in der Doku. Das reicht nicht – der **Einsatzzweck** bestimmt die Risikoklasse.

2 HR-Use-Case als „harmlos“ eingestuft

KI im Recruiting oder in der Leistungsbewertung ist **immer Hochrisiko**. Hier gibt es keinen Spielraum.

3 Keine Transparenzhinweise bei Chatbots

Jeder KI-Chatbot muss **klar kennzeichnen**, dass Nutzer:innen mit einer Maschine interagieren.

4 Keine Owner / Review-Daten

Ohne benannte Verantwortliche und Prüftermine ist Ihre Einstufung **nicht nachhaltig** und nicht auditfähig.

5 Kein Logging / keine Nachvollziehbarkeit

Ohne Protokollierung können Sie bei einer Prüfung nicht belegen, **wie und warum** Entscheidungen getroffen wurden.

✅ Quick-Check: 5 Ja/Nein-Fragen

Beantworten Sie diese Fragen für jeden Ihrer KI-Use-Cases. Jedes „Nein“ zeigt eine **Lücke** in Ihrer Compliance:

01

Use Case beschrieben?

Ist der konkrete Einsatzzweck (nicht nur der Tool-Name) dokumentiert?

02

Risikoklasse zugeordnet?

Wurde der Entscheidungsbaum durchlaufen und die Klasse festgelegt?

03

Pflichten abgeleitet?

Sind die konkreten ToDos pro Use Case definiert?

04

Owner benannt?

Gibt es eine verantwortliche Person mit Entscheidungskompetenz?

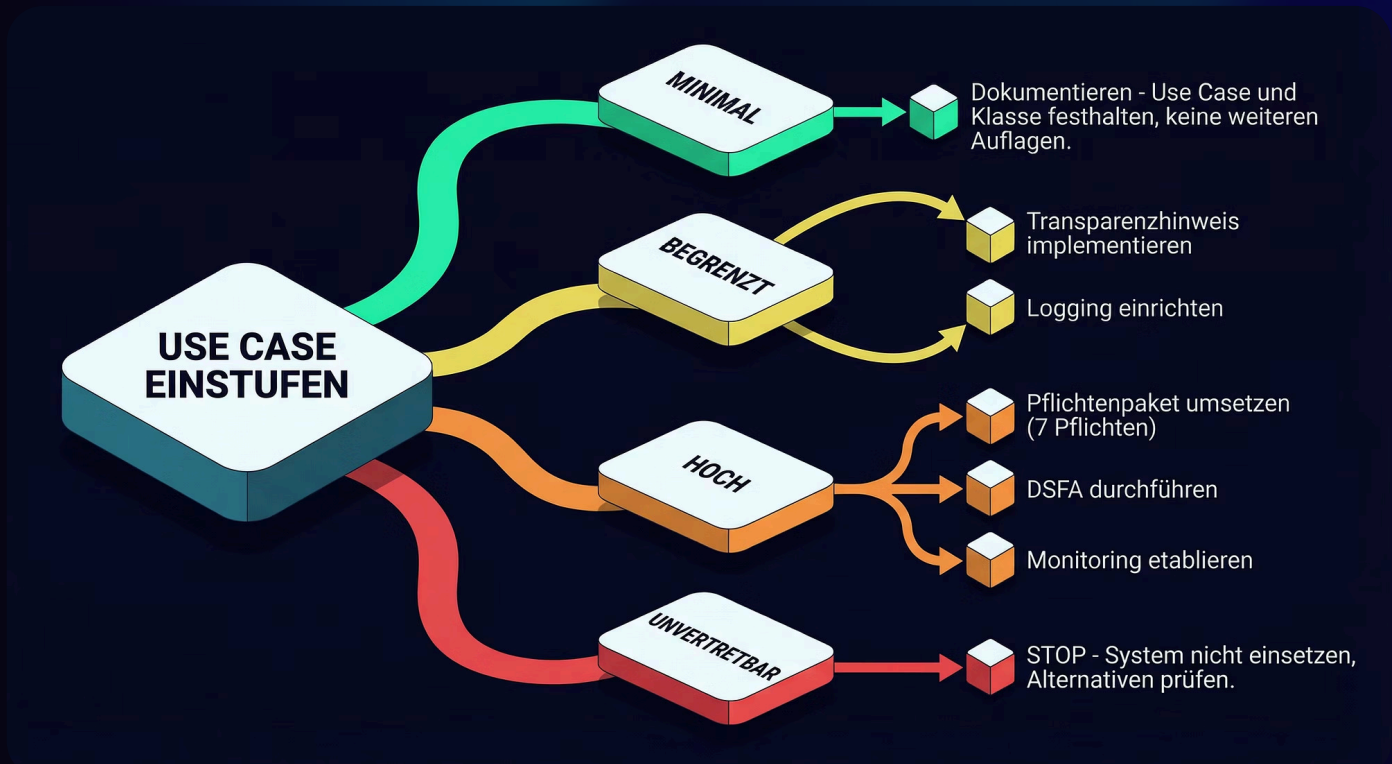
05

Review-Datum gesetzt?


Ist ein Termin zur Überprüfung innerhalb der nächsten 12 Monate geplant?

Mini-Workflow: Was mache ich nach der Einstufung?


Sie haben Ihren Use Case eingestuft – und jetzt? Die richtige Reaktion hängt direkt von der zugewiesenen Risikoklasse ab. Der folgende Workflow zeigt Ihnen den jeweils nächsten Schritt nach der Klassifikation. Vom einfachen Dokumentieren bei minimalen Risiken bis zum umfassenden Pflichtenpaket bei Hochrisiko-Systemen: Jede Klasse erfordert ein eigenes Maßnahmenbündel. Bei der Kategorie **Unvertretbar** gilt: Sofort stoppen und nach Alternativen suchen.




Minimal

 Dokumentieren und ablegen. Keine weiteren regulatorischen Auflagen erforderlich.


Begrenzt


 Transparenzhinweis + Logging implementieren. Nutzer:innen informieren.

Hoch

 Vollständiges Pflichtenpaket + DSFA + laufendes Monitoring einrichten.

Unvertretbar

 Sofort stoppen! System nicht einsetzen, Alternativen evaluieren.

 **Wichtig:** Die Einstufung ist kein einmaliger Vorgang. Ändern sich Einsatzzweck, Datenquellen oder betroffene Personengruppen, muss die Klassifikation überprüft werden. Planen Sie **regelmäßige Reviews** ein. Weitere Workflow-Templates auf www.kaffee-intelligenz.de.

Zeitplan & Fristen des EU AI Acts

Der AI Act wurde im August 2024 im EU-Amtsblatt veröffentlicht und tritt stufenweise in Kraft. Für KMU ist es entscheidend, die relevanten Fristen zu kennen und rechtzeitig Maßnahmen einzuleiten. Warten Sie nicht auf den letzten Moment – eine schrittweise Umsetzung ist nicht nur pragmatischer, sondern demonstriert auch gegenüber Kunden, Partnern und Behörden Ihre proaktive Haltung. Die folgende Übersicht zeigt die wichtigsten Meilensteine.



35M€

Maximales Bußgeld

bei Verstoß gegen Verbote

7%

Jahresumsatz

alternatives Bußgeldmaß

12

Monate

bis Hochrisiko-Pflichten greifen

Verantwortlichkeiten & Governance

Eine erfolgreiche AI-Act-Compliance steht und fällt mit klaren Verantwortlichkeiten. In vielen KMU fehlt eine dedizierte Compliance-Abteilung – umso wichtiger ist es, Zuständigkeiten explizit zu definieren und in bestehende Strukturen zu integrieren. Die Risiko-Matrix wird nur dann zum lebenden Dokument, wenn es Personen gibt, die sie pflegen, überprüfen und aktualisieren. Der folgende Rahmen zeigt, wie Sie mit minimalem Aufwand eine effektive Governance-Struktur aufbauen.



Geschäftsführung

Trägt die **Gesamtverantwortung** für AI-Act-Compliance. Gibt Budget frei, genehmigt Risikoklassen-Einstufungen und stellt sicher, dass Compliance in der Unternehmensstrategie verankert ist. Muss über Hochrisiko-Systeme informiert sein.



AI-Compliance-Beauftragte:r

Zentrale Koordinationsstelle für alle KI-bezogenen Compliance-Fragen. Pflegt die Risiko-Matrix, koordiniert Reviews, schult Mitarbeitende und ist Ansprechpartner:in für Behörden. In KMU oft in Personalunion mit Datenschutz.



Fachbereichs-Owner

Jeder KI-Use-Case benötigt einen **verantwortlichen Owner** aus dem jeweiligen Fachbereich. Diese Person kennt den Einsatzzweck, überwacht die Umsetzung der Pflichten und meldet Änderungen am Use Case.



Datenschutzbeauftragte:r

Unterstützt bei der **DSFA** (Datenschutzfolgenabschätzung) für Hochrisiko-Systeme, prüft die Rechtmäßigkeit der Datenverarbeitung und stellt die Verbindung zwischen DSGVO und AI Act her.

Best Practice: Richten Sie einen quartalsweisen „AI Compliance Review“ ein, bei dem alle Use-Case-Owner den Status ihrer Systeme berichten. So bleibt die Risiko-Matrix aktuell und Ihre Governance lebt. Mehr dazu auf www.kaffee-intelligenz.de.

KMU-Umsetzungsstrategie: Schritt für Schritt

Die Anforderungen des AI Acts können für KMU überwältigend wirken. Doch mit einer pragmatischen Umsetzungsstrategie lässt sich die Compliance schrittweise aufbauen – ohne den laufenden Betrieb zu gefährden. Der folgende Stufenplan zeigt Ihnen, wie Sie in vier Phasen vom Status quo zur vollständigen Compliance gelangen. Wichtig: Beginnen Sie jetzt, nicht erst kurz vor den Fristen. Frühzeitige Umsetzung verschafft Ihnen einen Wettbewerbsvorteil und reduziert das Risiko kostspieliger Nacharbeiten.

Phase 1: Inventur (Sofort)

Listen Sie **alle KI-Systeme und Use Cases** in Ihrem Unternehmen auf. Viele KMU sind überrascht, wie viele KI-Anwendungen bereits im Einsatz sind – von der automatischen E-Mail-Sortierung bis zur Bildbearbeitung. Nutzen Sie die Risiko-Matrix-Vorlage.

Phase 2: Klassifikation (Q3/2025)

Durchlaufen Sie den **Entscheidungsbaum** für jeden Use Case. Ordnen Sie Risikoklassen zu, benennen Sie Owner und setzen Sie Review-Termine. Identifizieren Sie sofort, ob verbotene Praktiken vorliegen.

Phase 3: Pflichten umsetzen (Q4/2025 – Q2/2026)

Arbeiten Sie die **Pflichtenliste** pro Use Case ab. Beginnen Sie mit Hochrisiko-Systemen: DSFA durchführen, Dokumentation erstellen, Logging implementieren, menschliche Aufsicht einrichten. Transparenzhinweise für begrenzte Systeme umsetzen.

Phase 4: Monitoring & Review (ab Q3/2026)

Etablieren Sie **dauerhafte Governance-Prozesse**: Quartalsweise Reviews, Incident-Reporting, Schulungen für neue Mitarbeitende und kontinuierliche Aktualisierung der Risiko-Matrix bei Änderungen an Systemen oder Einsatzzwecken.

60%

KMU ohne Inventur

haben noch keine Übersicht ihrer KI-Systeme

80%

Zeitersparnis

durch frühzeitige vs. Last-Minute-Umsetzung

4/4

Phasen

für vollständige Compliance bis August 2026

Branchenfokus: KI in der Kaffee- & Lebensmittelbranche

Die Kaffee- und Lebensmittelbranche setzt zunehmend auf KI – von der Lieferkette über die Qualitätssicherung bis zum Kundenservice. Für KMU in dieser Branche ergeben sich spezifische Anwendungsfälle, die eine differenzierte Betrachtung erfordern. Der AI Act trifft diese Unternehmen an vielen Stellen: Sensorbasierte Qualitätskontrollen, automatisierte Bestellprozesse, personalisierte Marketingkampagnen und KI-gestützte Personalplanung sind nur einige Beispiele. Die folgende Übersicht ordnet typische Use Cases der Branche ein.



Qualitätssicherung

Risikoklasse: Hoch (wenn qualitätsentscheidend)

Bildbasierte Bohnenauswahl, Sensoranalyse des Röstprofils, automatische Fehlererkennung. Diese Systeme beeinflussen direkt die Produktsicherheit und Verbrauchergesundheit.



Lieferketten-Tracking

Risikoklasse: Hoch (bei Entscheidungsrelevanz)

KI-gestützte Nachverfolgung von Rohstoffen, Lieferantenscoring, Prognosemodelle für Verfügbarkeit. Besonders relevant bei Fair-Trade- und Nachhaltigkeitszertifizierungen.



Kundenservice & Marketing

Risikoklasse: Begrenzt

Chatbots für Bestellstatus, KI-generierte Produktbeschreibungen, personalisierte Newsletter. Transparenzpflicht: Kund:innen müssen wissen, wann sie mit KI interagieren.

Die Besonderheit der Kaffee- und Lebensmittelbranche liegt in der engen Verzahnung von Qualitätssicherung, Verbraucherschutz und Lieferkettentransparenz. KI-Systeme, die in diesen Bereichen Entscheidungen treffen oder maßgeblich beeinflussen, werden in der Regel als Hochrisiko eingestuft. Planen Sie entsprechende Ressourcen für die Compliance ein und nutzen Sie branchenspezifische Umsetzungshilfen auf www.kaffee-intelligenz.de.

Ressourcen, Kontakt & Nächste Schritte

Sie haben die Grundlagen der AI-Act-Risikobewertung kennengelernt, Ihren Werkzeugkasten mit Entscheidungsbaum, Pflichtenkatalog und Risiko-Matrix gefüllt und konkrete Praxisbeispiele durchgearbeitet. Jetzt geht es an die Umsetzung. Dieses Playbook ist Teil einer umfassenden Ressourcensammlung, die Ihnen hilft, KI in Ihrem Unternehmen verantwortungsvoll und rechtskonform einzusetzen. Alle weiteren Materialien, Updates zum AI Act und interaktive Tools finden Sie auf der begleitenden Website.

Weiterführende Ressourcen

01

Buch: Kaffee & Künstliche Intelligenz

Der umfassende Leitfaden für KMU-Entscheider, die KI strategisch und compliant einsetzen möchten. Von Grundlagen über Anwendungsfälle bis zur Governance – praxisnah und verständlich aufbereitet.

02

Website & Templates

Auf www.kaffee-intelligenz.de finden Sie alle Templates aus diesem Playbook als editierbare Downloads, regelmäßige Updates zu AI-Act-Fristen und weitere Branchenbeispiele.

03

Newsletter & Community

Bleiben Sie auf dem Laufenden: Abonnieren Sie den monatlichen AI-Act-Update-Newsletter und tauschen Sie sich mit anderen KMU-Entscheider:innen aus.

Buch-Teaser



Kaffee & Künstliche Intelligenz

Wie KMU der Kaffeebranche KI strategisch nutzen, Risiken managen und den AI Act pragmatisch umsetzen. Ein Leitfaden von **Philipp Diekmann**.

Kontakt

Philipp Diekmann

www.kaffee-intelligenz.de

|