EU AI ACT DSGVO BDSG ISO/IEC 42001

Playbook #1

KI-Compliance in der Rösterei

In 7 Schritten von Tool-Dschungel zu prüfbar & sicher

KI ist längst Alltag in Röstereien – aber Verantwortung entsteht erst durch Struktur. Dieses Playbook führt dich in 7 Schritten zu einem Setup, das nachvollziehbar und auditierbar ist.

Version 1.0 | 2026 · Philipp Diekmann · kaffee-intelligenz.de

Ziel & Definition of Done

🎯 Ziel dieses Playbooks

- **Du weißt, welche KI-Systeme du im Betrieb nutzt** – inkl. Zweck, Daten und Owner.
- **Du hast Risiken nach EU AI Act grob klassifiziert** und Datenschutz geprüft.
- **Du hast Dokumentation, Schulung und Monitoring als Routine etabliert** – nicht als Einmalprojekt.

✅ Definition of Done

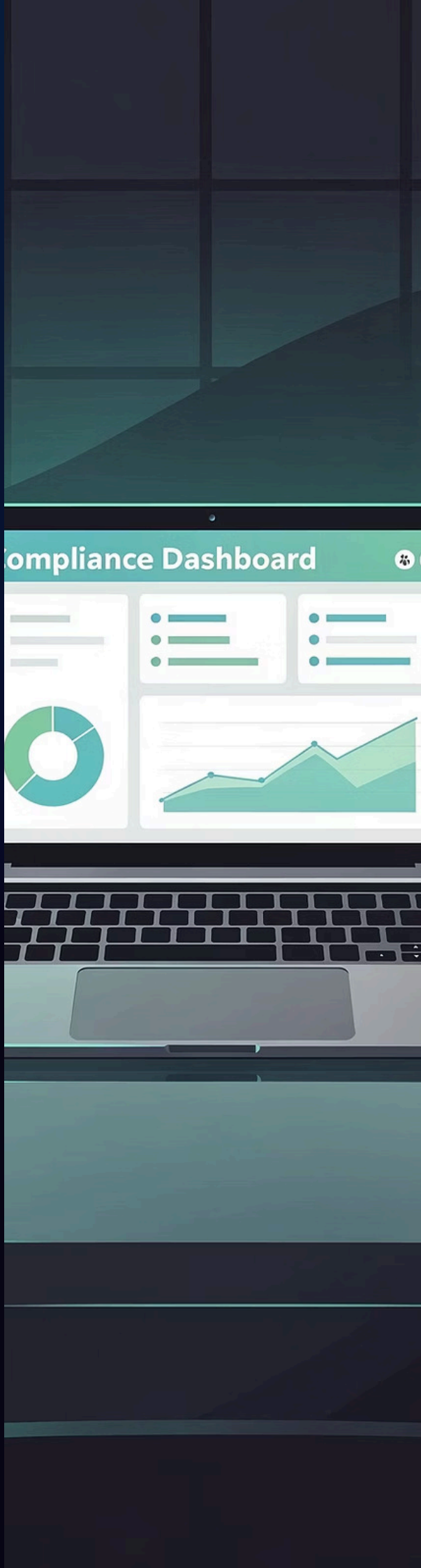
1. KI-Inventar vollständig

2. Risiko- & Datenschutz-Check dokumentiert

3. Rollen & Logbuch aktiv

4. Monitoring & Review-Rhythmus festgelegt

> *„Compliance ist kein Projekt, sondern ein Prozess – wie das kontinuierliche Röst-Tuning."*



Was bedeutet KI-Compliance im Alltag?

KI-Compliance umfasst alle Maßnahmen, mit denen du sicherstellst, dass KI im Unternehmen Gesetze und interne Regeln einhält – egal ob für Text, Planung, Qualitätsprüfung oder Marketing. Es geht nicht um Verbote, sondern um **Nachvollziehbarkeit und Verantwortung**. Jeder KI-Einsatz, der Entscheidungen beeinflusst oder personenbezogene Daten verarbeitet, braucht einen klaren Rahmen.

In der Kaffeebranche betrifft das weit mehr als nur Chatbots. Schon Prognosetools im ERP, automatische Bestellvorschläge oder sensorgestützte Röstprofile sind KI-Anwendungen, die unter regulatorische Anforderungen fallen können. Die gute Nachricht: Mit System und Struktur ist das machbar – auch für KMU.

Social Media Texte

z. B. ChatGPT, Gemini für Posts & Kampagnen

Preis- & Bestellvorschläge

Automatisierte Empfehlungen aus ERP/CRM

Röstprofile & Qualitätsanalyse

Sensor-basierte Steuerung & Auswertung

Lieferketten-Monitoring

Tracking, Prognosen & Risikoerkennung

💡 **Merksatz:** Was nachvollziehbar ist, ist auch verantwortbar.

Die 7 Schritte zur KI-Compliance

Der Weg zur prüfbaren KI-Nutzung ist kein Sprint, sondern ein strukturierter Prozess. Diese sieben Schritte bilden das Rückgrat deiner KI-Governance – vom ersten Überblick bis zum laufenden Monitoring. Jeder Schritt baut auf dem vorherigen auf und erzeugt konkrete, dokumentierbare Ergebnisse.

01

Inventur

Alles erfassen, was KI ist – inkl. Plugins, APIs und versteckte Features.

02

Klassifizierung

Risikoklasse nach EU AI Act festlegen – vom minimalen bis zum unvertretbaren Risiko.

03

Datenschutzprüfung

Datenarten & DSFA-Bedarf prüfen – personenbezogene Daten im Fokus.

04

Verantwortlichkeiten

Owner und AI Officer benennen – klare Zuständigkeiten schaffen.

05

Dokumentation

Logbuch & technische Dokumentation pflegen – Nachvollziehbarkeit sichern.

06

Schulung

Mitarbeitende befähigen – Pflicht nach Art. 4 AI Act.

07

Überwachung

Qualität & Risiken laufend überwachen – kontinuierliche Verbesserung.

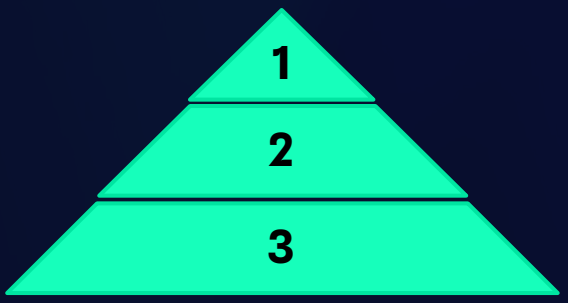
Schritt 1 – Inventur: Welche KI-Systeme nutzen wir?

Die Inventur ist das Fundament jeder KI-Compliance. Ohne ein vollständiges Bild darüber, welche KI-Systeme, -Features und -Schnittstellen im Einsatz sind, ist keine seriöse Risikobewertung möglich. Viele Unternehmen unterschätzen, wie viel KI bereits im Alltag steckt – oft versteckt in ERP-Modulen, Office-Tools oder Cloud-Services.

Was gehört ins Inventar?

- **Erfasse Tools, Plugins, APIs und Features** in Office/ERP, die KI enthalten – auch wenn sie „nur" Vorschläge machen.
- **Zähle auch Prognose- und Auto-Vorschläge** in ERP/CRM als KI-Funktionen. Ein Absatzprognose-Modul ist KI.
- **Ziel: Vollständigkeit, nicht Perfektion.** Besser 80 % erfasst und ergänzen als ewig auf 100 % warten.
- **Output: KI-Inventarliste** (Template siehe Ressourcen-Seite am Ende).

Inventory Funnel



1. **Inventarliste**
2. **KI-Tools & Features**
3. **Alle Tools im Betrieb**

📌 **Praxisbeispiel:** Eine Rösterei nutzt ChatGPT für Social Media Posts, ein Helpdesk-Tool mit Auto-Antworten und ein ERP mit Absatzprognose. Alle drei gehören ins Inventar – auch wenn nur eines „offensichtlich KI" ist.

Schritt 2 – Klassifizierung: Welches Risiko besteht?

Der EU AI Act teilt KI-Systeme in vier Risikokategorien ein. Die Einstufung bestimmt, welche Pflichten du hast – von „keine besonderen Auflagen" bis hin zu einem vollständigen Verbot. Für die Kaffeebranche ist diese Einordnung essenziell, weil viele Tools auf den ersten Blick harmlos wirken, aber je nach Einsatzkontext in eine höhere Kategorie rutschen können.

Risikokategorie	Beschreibung	Beispiel Kaffeebranche	Praktische Folge
🔴 Unvertretbar	Manipuliert Menschen oder verletzt Grundrechte	Emotionserkennung am Arbeitsplatz	**Verbot**
🟠 Hoch	Einfluss auf sicherheits- oder rechtsrelevante Entscheidungen	Bewerberauswahl, Qualitätsanalyse, Lieferketten-Tracking	**Strenge Pflichten**
🔵 Begrenzt	Informations- und Transparenzpflicht	Chatbots, Marketing-KI	**Hinweis: „KI im Einsatz"**
🟢 Minimal	Geringfügige Unterstützung	Filter, Textvorschläge	**Keine besonderen Auflagen**

⚠️ Merke: Kontext zählt.

Ein und dasselbe Tool kann je nach Einsatzkontext in unterschiedliche Risikokategorien fallen. Entscheidend ist nicht die Technologie, sondern der Zweck.

💡 Beispiel

Chatbot auf der Website = begrenztes Risiko → Kennzeichnungspflicht. Derselbe Chatbot intern für HR-Entscheidungen = potenziell hohes Risiko.

Schritt 3 – Datenschutzprüfung: Welche Daten verarbeitet das System?

Datenschutz ist das zweite große Compliance-Thema neben dem AI Act. Sobald personenbezogene Daten ins Spiel kommen – und das passiert schneller als gedacht – greifen DSGVO und BDSG. Die Datenschutzprüfung hilft dir, den tatsächlichen Schutzbedarf jedes KI-Systems einzuschätzen und die richtigen Maßnahmen abzuleiten.

Checkliste Datenschutz

- **Personenbezogene Daten?**

  Name, E-Mail, Telefonnummer, Kundendaten

- **Sensible Daten / Profiling?**

  Verhalten, Vorlieben, Kaufmuster

- **Automatisierte Entscheidungen?**

  Mit Wirkung auf Personen (Art. 22 DSGVO)

- **Drittlandtransfer / Cloud außerhalb EU?**

  Serverstandort & Datenverarbeitung prüfen

- **Speicherung von Prompts/Inputs?**

  Werden Eingaben beim Anbieter gespeichert?

- **Daten für KI-Training genutzt?**

  Opt-out-Optionen prüfen

Entscheidungslogik

Hohes Risiko / Profiling / HR

→ DSFA / Privacy Review erforderlich. Vollständige Datenschutz-Folgenabschätzung durchführen.

Personenbezogen, geringes Risiko

→ DSFA-Light + technisch-organisatorische Maßnahmen (TOMs) umsetzen.

Keine personenbezogenen Daten

→ DSFA meist nicht nötig – trotzdem dokumentieren!

⚖️ **Rechtlicher Hinweis:** Wenn personenbezogene Daten betroffen sind: DSGVO (u. a. Art. 5, Art. 22) und BDSG (§ 26 bei Beschäftigtendaten) beachten. Im Zweifel: Datenschutzbeauftragte:n einbinden.

Schritt 4 – Verantwortlichkeiten: Wer ist zuständig?

KI-Compliance funktioniert nur, wenn klar ist, wer Entscheidungen trifft, wer dokumentiert und wer eskaliert. In vielen KMU der Kaffeebranche gibt es keine eigene IT-Abteilung – umso wichtiger ist ein pragmatisches Rollenmodell, das zu eurer Betriebsgröße passt. Die Benennung einer verantwortlichen Person ist keine Kür, sondern Pflicht für einen verlässlichen Betrieb.

Das Organigramm zeigt die idealtypische Struktur – in der Praxis werden Rollen häufig kombiniert. Wichtig ist nicht die Anzahl der Personen, sondern die Klarheit der Zuständigkeiten.

Verantwortliche Person benennen

Eine klare Zuordnung ist Pflicht für verlässlichen KI-Betrieb – auch wenn es „nur" eine Teilzeitrolle ist.

Kombinierte Rollen in KMU

Oft übernimmt eine Person IT + Datenschutz + Fachbereich. Das ist okay – solange es dokumentiert ist.

Freigabe- & Eskalationswege

Definiere klar, wer neue KI-Tools freigibt und an wen bei Problemen eskaliert wird.

Review-Rhythmus festlegen

Monatlich oder vierteljährlich – ein fester Termin sorgt dafür, dass Compliance kein Papiertiger bleibt.

Schritt 5 – Dokumentation: Wie funktioniert das System?

Dokumentation ist das Rückgrat jeder Compliance-Struktur. Ohne sie gibt es keine Nachvollziehbarkeit, keine Auditierbarkeit und im Ernstfall keine Verteidigung. Das Gute: Es geht nicht um Bürokratie, sondern um ein schlankes System, das mitläuft. Ein KI-Logbuch erfasst alle relevanten Änderungen, Entscheidungen und Prüfungen an einem zentralen Ort.

Dokumentationsprinzipien

- **Führe ein KI-Logbuch** – Änderungen, Prompts, Modelle und Datenquellen gehören rein.
- **Dokumentiere Zweck, Nutzung, Datenquellen** und eingesetzte Modelle für jedes System.
- **Hinterlege Prüf- und Freigabeschritte** – wer hat wann was genehmigt?
- **Ziel: Nachvollziehbarkeit, nicht Bürokratie.** Lieber schlank und gepflegt als umfangreich und veraltet.

KI-Logbuch – Mindestfelder

- 📅 **Datum**
- 🎯 **Use Case**
- 🔄 **Change-Typ**
  Prompt / Modell / Daten / Policy
- 📝 **Beschreibung**
- ⚠️ **Risiko-Auswirkung**
- ✅ **Test / Validierung**
- 👤 **Freigabe durch**
- 🔁 **Nächster Review**

💡 **Tipp:** Starte mit einer einfachen Tabelle (z. B. in Notion, Excel oder Google Sheets). Perfektion ist der Feind des Anfangs – Hauptsache, das Logbuch existiert und wird gepflegt.

Schritt 6 – Schulung: Wer nutzt die Systeme?

Alle Mitarbeitenden, die KI bedienen oder Ergebnisse bewerten, müssen geschult sein. Das ist nicht nur Best Practice, sondern nach Art. 4 des EU AI Acts eine Pflicht. Schulungen müssen dokumentiert werden und regelmäßig aufgefrischt – denn KI-Systeme verändern sich, und damit auch die Anforderungen an die Nutzenden.

Schulungsplan – Minimal

Ziel-gruppe	Lernziele	Inhalte	Format	Dauer	Nachweis	Refresh
Marketing / Kommu-nikation	Saubere Prompts, Quellen, Claims vermei-den	Prompt-Basics, Halluzinationen, Datenschutz, Tonalität	Work-shop	2h	Teilnahme liste	Jähr-lich
QS / Produk-tion	KI-Ergeb-nisse kritisch bewerten	Bias, Datenqualität, Ausreißer, Freigabe-prozess	Training-on-the-job	2h	Check-liste bestan-den	Jähr-lich
Führung / Owner	Risiko & Gover-nance steuern	Risikoklassen, DSFA-Light, Logbuch, Incident-Prozess	Briefing	1h	Protokoll	Halbjährlich

Der Schulungsplan ist bewusst schlank gehalten. In einer typischen Rösterei mit 15–50 Mitarbeitenden lässt sich das Programm innerhalb von zwei Wochen ausrollen. Wichtig: Dokumentiere jeden Schulungstermin mit Datum, Teilnehmenden und behandelten Themen – das ist im Auditfall Gold wert.

Schritt 7 – Überwachung: Wie bleibt KI zuverlässig?

KI-Systeme verändern sich – durch Updates, neue Daten oder veränderte Nutzungsmuster. Deshalb endet Compliance nicht mit der Einführung, sondern beginnt dort erst richtig. Kontinuierliches Monitoring stellt sicher, dass deine KI-Systeme zuverlässig, fair und rechtskonform bleiben. Ein einfaches Dashboard mit vier KPIs gibt dir jederzeit den Überblick.

Monitoring-Dashboard: 4 KPIs

Output-Qualität

Stichproben-Score: Werden die Ergebnisse regelmäßig geprüft und bewertet?

Drift / Änderungen

Neue Daten, Tool-Updates oder Modellwechsel – alles, was die Ergebnisse beeinflusst.

Incidents

Anzahl und Schwere von Vorfällen: fehlerhafte Outputs, Beschwerden, Datenpannen.

Adoption

Nutzungsgrad und Feedback der Mitarbeitenden – wird das System akzeptiert und richtig genutzt?

Post-Deployment Review (nach 4 Wochen)

Vier Wochen nach Einführung eines neuen KI-Systems oder eines größeren Updates solltest du eine strukturierte Überprüfung durchführen:

1

Qualität stabil?

Sind die Ergebnisse konsistent und auf dem erwarteten Niveau?

2

Beschwerden / Fehlentscheidungen?

Gab es Rückmeldungen von Kunden oder Mitarbeitenden?

3

Datenschutz / Logs ok?

Werden personenbezogene Daten wie geplant verarbeitet?

4

Dokumentation aktuell?

Prompt-/Modellversion im Logbuch dokumentiert?

5

Schulungsbedarf?

Zeigen sich Wissenslücken oder neue Anforderungen?

6

Verbesserungen priorisiert?

Nächste Optimierungen identifiziert und eingeplant?

Zusammenfassung: Dein Compliance-Kompass

Du hast jetzt alle sieben Schritte durchlaufen – von der ersten Inventur bis zum laufenden Monitoring. Hier noch einmal der Gesamtüberblick, damit du jederzeit weißt, wo du stehst und was als Nächstes kommt. Die Prozentwerte zeigen den typischen Aufwand pro Schritt in einem KMU-Setup.

Inventur

Alle KI-Systeme erfasst

Klassifizierung

Risikostufen zugeordnet

Schulung

Team befähigt & dokumentiert

Datenschutz

DSGVO-Check dokumentiert

Dokumentation

Logbuch & Doku aktiv

Verantwortung

Rollen & Owner benannt

> *„KI-Compliance ist kein Einmal-Event. Es ist eine Haltung – und diese Haltung beginnt mit dem ersten dokumentierten Schritt."*

Quick Win

Starte heute mit der Inventur. 30 Minuten reichen für den ersten Überblick.

Nächster Meilenstein

Setze dir ein Datum für den ersten Review – in 4 Wochen.

Langfristig

Integriere den 7-Schritte-Zyklus in dein Quartals-Reporting.

Auf einen Blick: Deine Compliance-Reife

Wo steht deine Rösterei? Nutze diese Selbsteinschätzung, um deinen aktuellen Stand zu bewerten und Handlungsfelder zu priorisieren. Jeder Schritt, der auf „Erledigt" steht, ist ein Baustein für ein auditierbares KI-Setup.

Stufe 1: Bewusstsein

KI-Nutzung ist bekannt, aber nicht systematisch erfasst. Der erste Schritt – Inventur – steht noch aus.

Stufe 2: Struktur

Inventar, Klassifizierung und Datenschutzprüfung sind abgeschlossen. Grundlagen stehen.

Stufe 3: Routine

Rollen sind besetzt, Logbuch wird gepflegt, erste Schulungen durchgeführt.

Stufe 4: Reife

Alle 7 Schritte implementiert, Monitoring läuft, regelmäßige Reviews finden statt.

Egal auf welcher Stufe du gerade stehst: Jeder Schritt nach vorne zählt. Compliance ist kein Alles-oder-Nichts – es ist ein kontinuierlicher Weg. Die Tatsache, dass du dieses Playbook gelesen hast, zeigt, dass du auf dem richtigen Weg bist.

🎯 **Empfehlung:** Plane einen halben Tag pro Quartal für einen Compliance-Check ein. Mit dem 7-Schritte-Framework hast du die Struktur dafür.

Ressourcen & Kontakt

Auf **kaffee-intelligenz.de** findest du weitere Playbooks, Templates und Praxisbeispiele rund um KI in der Kaffeebranche – pragmatisch, sofort umsetzbar und mit Fokus auf Verantwortung. Dieses Playbook ist der Anfang – nicht das Ende.

Kontakt & Austausch

✉️ E-Mail

philipp@kaffee-intelligenz.de

🌐 Web

kaffee-intelligenz.de

💼 LinkedIn

linkedin.com/in/philippdiekmann

Über den Autor

Philipp Diekmann ist Kaffeeexperte mit rund zwei Jahrzehnten Praxis – und spezialisiert auf KI-Governance, Automatisierung und verantwortungsvolle Implementierung im Betriebsalltag. Er verbindet tiefes Branchenwissen mit technologischer Kompetenz und begleitet Röstereien und Kaffeeproduzenten auf dem Weg zu einem strukturierten KI-Einsatz.

Buch-Tipp: Kaffee Intelligenz

Kaffee Intelligenz zeigt dir, wie du Künstliche Intelligenz in der Kaffeebranche verstehst, anwendest und verantwortungsvoll betreibst – von den Grundlagen über Recht & Governance bis zu Nachhaltigkeit, Marketing und Zukunftsszenarien.

Du bekommst praxisnahe Beispiele, klare Entscheidungslogiken und einen Werkzeugkasten, der KMU wirklich hilft: weniger Tool-Chaos, mehr Wirkung im Alltag.

Das Buch richtet sich an Inhaber:innen, Führungskräfte und Macher:innen, die KI nicht nur testen, sondern sauber einführen und stabil betreiben wollen.