AI GOVERNANCE TEMPLATE

Template – KI-Logbuch (AI Governance Log)

Änderungen, Prompts, Modelle, Daten und Freigaben nachvollziehbar dokumentieren

Philipp Diekmann · kaffee-intelligenz.de

Zweck & Definition of Done

Das KI-Logbuch ist das zentrale Instrument für die lückenlose Dokumentation aller Änderungen an KI-Systemen in Ihrer Organisation. Es dient als Single Source of Truth für Betrieb, Audit, Übergaben und Compliance-Nachweise. In einer Welt, in der Regulierungen wie der EU AI Act konkrete Nachvollziehbarkeit fordern, ist ein strukturiertes Logbuch nicht optional – es ist Pflicht.

> *„Nachvollziehbarkeit für Betrieb, Audit, Übergaben. Jede Änderung hat Version, Beschreibung, Freigabe."*

Zweck des Logbuchs

Das Logbuch erfüllt mehrere kritische Funktionen gleichzeitig. Es schafft Transparenz über den gesamten Lebenszyklus eines KI-Use-Cases, ermöglicht schnelle Fehleranalyse bei Incidents und liefert die notwendige Dokumentation für interne und externe Audits. Darüber hinaus sichert es Wissenstransfer bei Personalwechseln und bietet eine klare Entscheidungsgrundlage für Rollbacks.

Jede Änderung – ob Prompt-Anpassung, Modellwechsel oder Datenquellenupdate – wird mit Version, Beschreibung und Freigabe erfasst. So entsteht ein vollständiges Bild der Systemevolution.

Definition of Done ✅

1. **Logbuch existiert**

   Jeder Use Case hat ein eigenes, aktiv gepflegtes Logbuch.

2. **Dokumentiert & getestet**

   Jede Änderung ist vollständig dokumentiert und vor Deployment getestet.

3. **Review-Rhythmus definiert**

   Feste Review-Zyklen sind vereinbart und werden eingehalten.

Was wird geloggt?

Das KI-Logbuch erfasst sechs zentrale Kategorien, die gemeinsam ein vollständiges Bild jeder KI-Systemänderung ergeben. Diese Kategorien bilden das Rückgrat der Dokumentation und stellen sicher, dass keine relevante Dimension übersehen wird – von der initialen Use-Case-Definition bis zur Incident-Dokumentation.

Jede Kategorie enthält spezifische Informationen, die für Audit-Sicherheit und operative Nachvollziehbarkeit unverzichtbar sind. Die konsistente Erfassung aller sechs Bereiche gewährleistet, dass Ihr Governance-Framework auch unter regulatorischem Druck standhält.

Use Case

Identifikation des KI-Anwendungsfalls, z. B. Support-Chatbot, Klassifikation, Empfehlungssystem

Prompt-Version

Versionierung aller Prompt-Änderungen, z. B. v1.2 → v1.3 mit Diff-Beschreibung

Modellwechsel

Dokumentation von Modell- und Anbieter-Updates inkl. Leistungsvergleich

Datenquellen

Erfassung aller genutzten Datenquellen: CRM, Tickets, Röstsensoren, FAQs etc.

Freigaben

Wer hat freigegeben? Owner, SteerCo oder andere autorisierte Stellen

Incidents

Dokumentation von Fehlern, Datenproblemen, Bias-Vorfällen und Gegenmaßnahmen

💡 **Praxistipp:** Beginnen Sie mit den Kategorien, die für Ihren wichtigsten Use Case am relevantesten sind. Erweitern Sie die Dokumentation schrittweise, statt alles auf einmal einzuführen.

Logbuch-Tabelle – Das Template

Die folgende Tabelle ist das Kernstück Ihres KI-Logbuchs. Sie enthält alle relevanten Spalten, um Änderungen lückenlos und auditfähig zu dokumentieren. Nutzen Sie diese Vorlage als Ausgangspunkt und passen Sie sie bei Bedarf an Ihre organisationsspezifischen Anforderungen an. Wichtig ist, dass jede Zeile eine einzelne, atomare Änderung repräsentiert – keine Sammeleinträge.

Die Spaltenstruktur wurde so konzipiert, dass sie den Anforderungen des EU AI Act, gängiger ISO-Standards und interner Audit-Prozesse entspricht. Besonderes Augenmerk liegt auf der Rückverfolgbarkeit: Von der Änderung über den Test bis zur Freigabe und dem nächsten Review-Termin ist jeder Schritt abgebildet.

Datum	Use Case	Change-Typ	Version alt → neu	Beschreibung	Grund	Risiko-Auswirkung	Test / Validierung	Freigabe durch	Rollback	Owner	Nächster Review
TT. MM. JJ	–	Prompt / Modell / Daten / Policy	vX.X → vX.X	–	–	–	–	–	Ja / Nein	–	TT. MM. JJ

Change-Typ Kategorien

Prompt – Jede Anpassung an System- oder User-Prompts
Modell – Wechsel des AI-Modells oder Anbieter-Updates
Daten – Neue, geänderte oder entfernte Datenquellen
Policy – Änderungen an Governance-Regeln oder Richtlinien

Rollback-Dokumentation

Für jede Änderung muss klar sein, ob ein Rollback möglich ist. Falls ja: Wo liegt die vorherige Version? Wie schnell kann zurückgerollt werden? Diese Information ist im Incident-Fall geschäftskritisch.

Beispiel-Einträge

Die folgenden drei Beispielzeilen zeigen, wie das Logbuch in der Praxis befüllt wird. Sie decken die häufigsten Change-Typen ab: Prompt-Änderung, Modellupdate und Datenquellenerweiterung. Nutzen Sie diese Einträge als Orientierung für Ihre eigene Dokumentation.

1️⃣ Prompt-Änderung: Support-Chatbot

Datum	Use Case	Change-Typ	Version	Beschreibung	Grund	Risiko	Test	Freigabe	Rollback	Owner	Review
12.03.25	Support-Bot	Prompt	v1.1 → v1.2	Antworten kürzer + Eskalationssatz ergänzt	Kundenfeedback	Gering	50 Tickets Eval-Set	Owner	Ja	M. Schmidt	12.04.25

2️⃣ Modellupdate: Anbieter-Migration

Datum	Use Case	Change-Typ	Version	Beschreibung	Grund	Risiko	Test	Freigabe	Rollback	Owner	Review
28.03.25	Support-Bot	Modell	GPT-4o → GPT-4.1	Anbieter-Update übernommen	Leistung + Kosten	Ton-Drift	Eval-Set bestanden	SteerCo	Ja	M. Schmidt	28.04.25

3️⃣ Datenquelle erweitert: FAQ-Integration

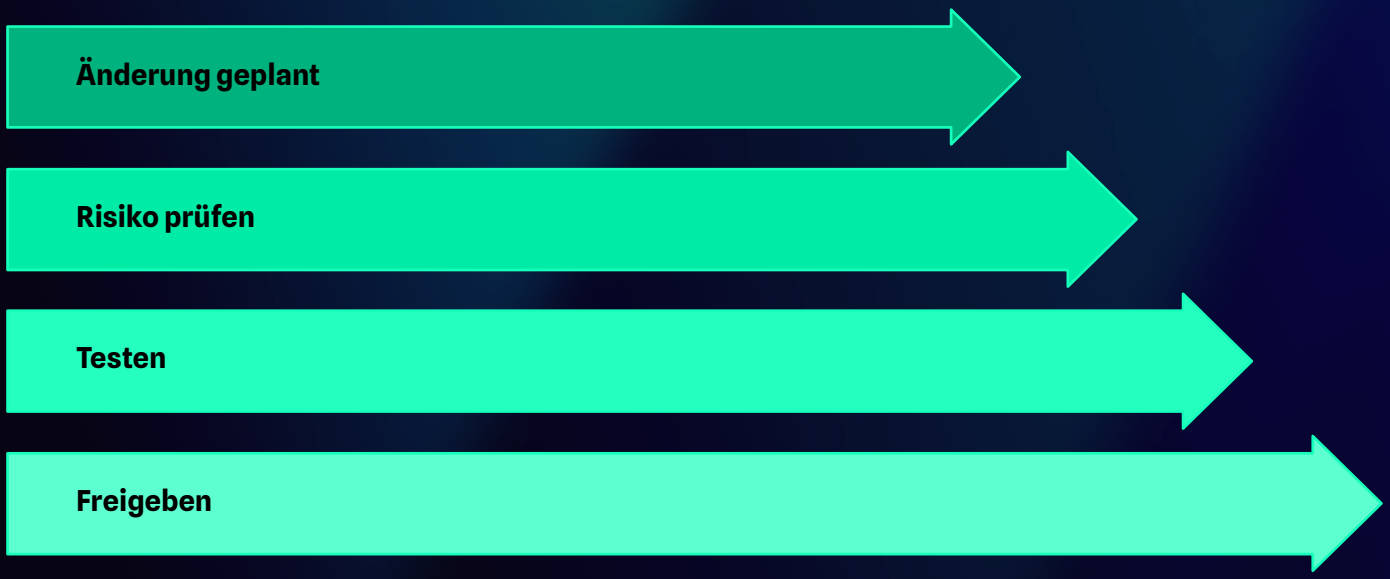
Datum	Use Case	Change-Typ	Version	Beschreibung	Grund	Risiko	Test	Freigabe	Rollback	Owner	Review
05.04.25	Support-Bot	Daten	DS v2 → v3	FAQ-Datenbank neu angebunden	Abdeckung erhöhen	Veraltete Infos	Stichprobe 30 Fragen	Owner	Ja	L. Weber	05.05.25

📋 **Hinweis:** Achten Sie darauf, dass jeder Eintrag atomar ist – eine Zeile pro Änderung. Kombinieren Sie niemals mehrere Changes in einer Zeile, auch wenn sie zeitgleich stattfinden.

Mini-Prozess: Wie wird geloggt?

Der Logging-Prozess ist bewusst schlank gehalten, damit er im Tagesgeschäft nicht zur Last wird. Sieben klar definierte Schritte stellen sicher, dass jede Änderung kontrolliert, getestet und dokumentiert in Produktion geht. Dieser Prozess gilt für alle Change-Typen – unabhängig davon, ob es sich um eine kleine Prompt-Anpassung oder einen vollständigen Modellwechsel handelt.

Entscheidend ist die Reihenfolge: Kein Deployment ohne vorherige Risikoprüfung und Test. Kein Test ohne dokumentierten Eval-Set. Keine Freigabe ohne klare Verantwortlichkeit. Das Logbuch wird **nach** dem erfolgreichen Deploy aktualisiert – nicht vorher, um nur tatsächlich durchgeführte Änderungen zu erfassen.



Dieser Prozess schützt Ihr Team vor unkontrollierten Änderungen und schafft die Grundlage für regulatorische Compliance. In der Praxis hat sich gezeigt, dass Teams, die diesen Prozess konsequent einhalten, deutlich weniger Incidents verzeichnen und schneller auf Probleme reagieren können.

1	**Änderung geplant** Änderungsbedarf identifizieren, Scope definieren, verantwortliche Person benennen.
2	**Risiko kurz prüfen** Schnelle Einschätzung: Welche Auswirkungen hat die Änderung? Ist ein Rollback möglich?
3	**Testen (Eval-Set)** Änderung gegen definiertes Eval-Set validieren. Ergebnisse dokumentieren.
4	**Freigeben** Owner oder SteerCo gibt formal frei. Freigabe wird im Logbuch vermerkt.
5	**Deploy** Änderung in Produktion bringen. Monitoring aktivieren.
6	**Logbuch aktualisieren** Alle Felder der Logbuch-Tabelle ausfüllen. Vollständigkeit prüfen.
7	**Review planen** Nächsten Review-Termin festlegen und im Kalender verankern.

Quick-Check: Ist Ihr Logbuch audit-ready?

Bevor Sie Ihr KI-Logbuch als „fertig" betrachten, sollten Sie die folgenden fünf Kernfragen mit einem klaren **Ja** beantworten können. Jede Frage adressiert einen kritischen Aspekt der KI-Governance, der bei Audits regelmäßig geprüft wird. Ein einziges „Nein" identifiziert eine Lücke, die zeitnah geschlossen werden sollte.

Dieser Quick-Check eignet sich sowohl für die initiale Einrichtung als auch für regelmäßige Selbst-Audits. Führen Sie ihn mindestens quartalsweise durch – oder nach jeder größeren organisatorischen Änderung.

01

Gibt es für jeden Use Case einen Owner?

Jeder KI-Use-Case braucht eine klar benannte verantwortliche Person, die für Dokumentation, Freigaben und Review zuständig ist. Ohne Owner gibt es keine Accountability – und ohne Accountability kein funktionierendes Governance-Framework. Prüfen Sie: Ist der Owner namentlich dokumentiert? Ist die Stellvertretung geregelt?

02

Sind Versionen nachvollziehbar?

Können Sie für jeden Prompt, jedes Modell und jede Datenquelle die aktuelle und alle vorherigen Versionen benennen? Versionierung ist die Grundlage für Rollback-Fähigkeit und Audit-Trails. Nutzen Sie semantische Versionierung (v1.0, v1.1, v2.0) für Klarheit.

03

Gibt es Tests vor jedem Deploy?

Kein Change darf ohne vorherige Validierung live gehen. Definieren Sie Eval-Sets für jeden Use Case und dokumentieren Sie Testergebnisse im Logbuch. Automatisierte Tests sind ideal, aber auch manuelle Stichproben sind besser als gar keine Prüfung.

04

Sind Freigaben dokumentiert?

Jede Änderung braucht eine formale Freigabe – ob durch den Owner, das SteerCo oder eine andere autorisierte Stelle. Die Freigabe muss im Logbuch mit Name und Datum erfasst sein. Mündliche Freigaben gelten für Audits nicht.

05

Gibt es eine Rollback-Option?

Für jede produktive Änderung muss klar sein: Kann sie rückgängig gemacht werden? Wie schnell? Wo liegt die vorherige Version? Ein fehlender Rollback-Plan ist ein hohes operatives Risiko, das bei Incidents zu langen Ausfallzeiten führen kann.

🎯 **Ziel:** 5 von 5 mit **Ja** beantwortet. Bei jedem „Nein" sofort eine Maßnahme definieren und im Logbuch als Policy-Change dokumentieren.

Governance-Reife: Wo stehen Sie?

Die Einführung eines KI-Logbuchs ist kein einmaliges Projekt, sondern ein kontinuierlicher Reifeprozess. Die meisten Organisationen durchlaufen dabei typische Stufen – von der reaktiven Ad-hoc-Dokumentation bis zur vollständig automatisierten Governance. Nutzen Sie das folgende Reifegradmodell, um Ihren aktuellen Stand einzuschätzen und gezielt die nächste Stufe anzusteuern.

Stufe 1: Ad-hoc

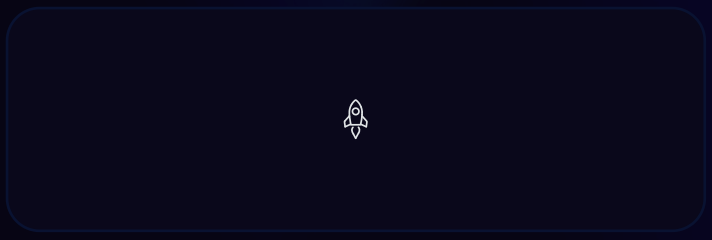
Keine systematische Dokumentation. Änderungen werden informell kommuniziert. Wissen liegt in den Köpfen einzelner Personen.

Stufe 2: Initial

Logbuch existiert als Vorlage. Erste Use Cases werden dokumentiert. Owner sind benannt, aber Prozesse noch nicht verbindlich.

Stufe 3: Definiert

Standardisierter Prozess für alle Use Cases. Eval-Sets definiert. Review-Rhythmus wird eingehalten. Quick-Check regelmäßig durchgeführt.



Stufe 4: Optimiert

Automatisierte Logging-Pipelines. Dashboards für Governance-KPIs. Proaktive Risikoerkennung. Vollständige Audit-Readiness jederzeit gegeben.

Typische Herausforderungen

- Fehlende Verbindlichkeit in der Anfangsphase
- Keine klare Zuordnung von Verantwortlichkeiten
- Eval-Sets sind nicht definiert oder veraltet
- Review-Termine werden verschoben oder vergessen
- Logbuch wird als bürokratische Last empfunden

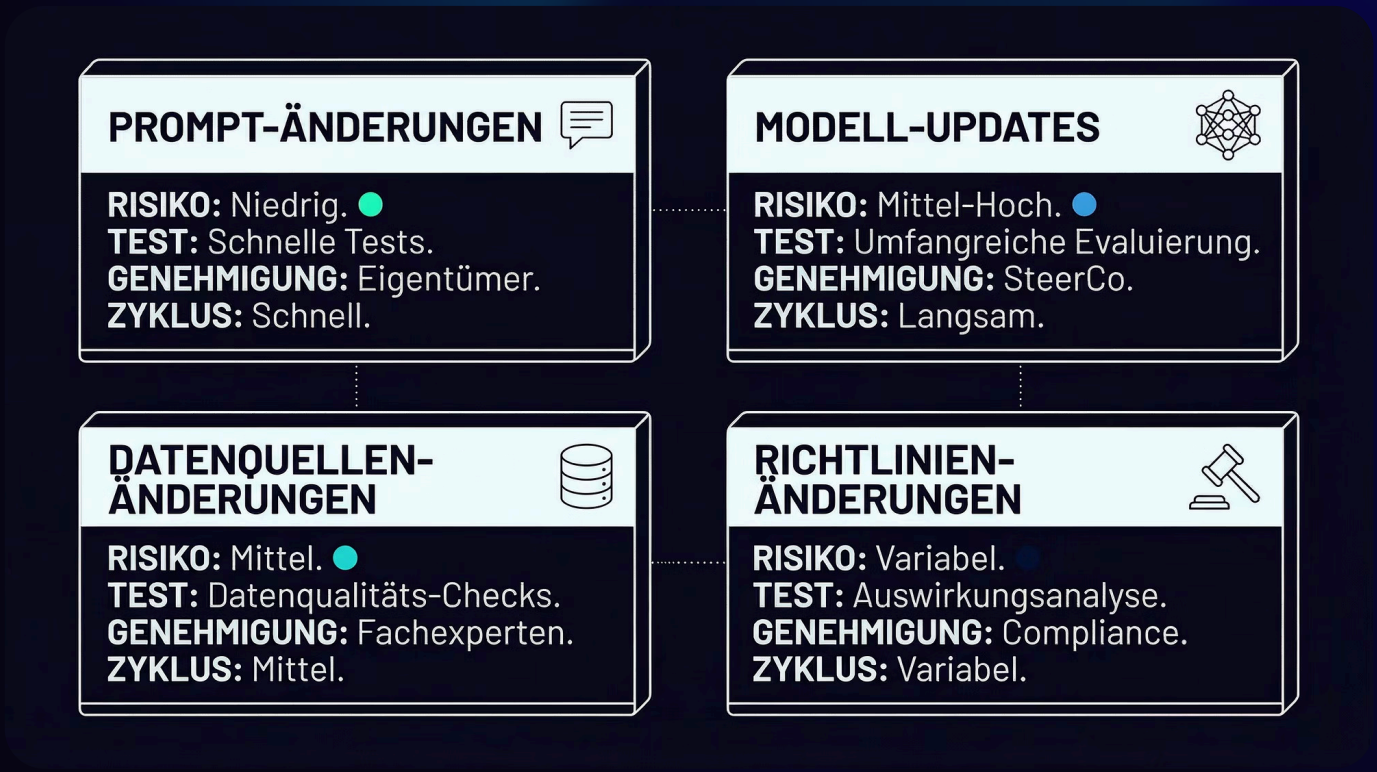
Erfolgsfaktoren

- Management-Commitment und Vorbildfunktion
- Integration in bestehende CI/CD-Prozesse
- Automatisierung wo möglich, manuell wo nötig
- Regelmäßiges Feedback aus Audits nutzen
- Logbuch als Enabler kommunizieren, nicht als Kontrolle

Philipp Diekmann · kaffee-intelligenz.de

Risiko-Matrix: Change-Typen im Vergleich

Nicht jede Änderung an einem KI-System birgt das gleiche Risiko. Ein kleines Prompt-Tuning hat andere Auswirkungen als ein kompletter Modellwechsel oder eine neue Datenquelle. Die folgende Übersicht hilft Ihnen, den angemessenen Prüf- und Freigabeaufwand für jeden Change-Typ festzulegen und so Ihre Governance-Ressourcen effizient einzusetzen.



Die Differenzierung nach Change-Typ ermöglicht es Ihnen, schlanke Prozesse für Low-Risk-Änderungen beizubehalten und gleichzeitig bei kritischen Changes die notwendige Sorgfalt walten zu lassen. Dokumentieren Sie die Risikoeinstufung als Teil Ihrer Governance-Policy und verweisen Sie im Logbuch darauf.

🟢 Prompt

Risiko: Gering bis Mittel
Freigabe: Owner
Review: Monatlich

🟠 Modell

Risiko: Mittel bis Hoch
Freigabe: SteerCo
Review: Nach Deploy + 2 Wochen

🟡 Daten

Risiko: Mittel
Freigabe: Owner + Daten-Team
Review: Monatlich

🔴 Policy

Risiko: Variabel
Freigabe: SteerCo
Review: Quartalsweise

Philipp Diekmann · kaffee-intelligenz.de

Review-Rhythmus & KPIs

Ein Logbuch ohne feste Review-Zyklen verliert schnell an Relevanz. Definieren Sie klare Zeitpunkte, an denen die Logbuch-Einträge auf Vollständigkeit, Aktualität und Korrektheit geprüft werden. Die folgenden KPIs helfen Ihnen, die Qualität Ihrer KI-Governance messbar zu machen und kontinuierlich zu verbessern.

Dokumentationsquote

Anteil der Changes mit vollständigem Logbuch-Eintrag

Test-Coverage

Anteil der Changes mit dokumentierter Validierung vor Deploy

Rollback-Readiness

Anteil der Changes mit bestätigter Rollback-Option

Review-Einhaltung

Anteil der Reviews, die termingerecht durchgeführt wurden

Empfohlene Review-Zyklen

🔄 Monatlich

Vollständigkeitscheck aller Logbuch-Einträge. Sind alle Changes des Monats erfasst? Sind Review-Termine aktuell? Gibt es offene Incidents?

📊 Quartalsweise

KPI-Auswertung und Trend-Analyse. Governance-Reifegrad bewerten. Policy-Änderungen prüfen. Ergebnisse an SteerCo berichten.

📋 Halbjährlich

Umfassender Audit-Readiness-Check. Eval-Sets auf Aktualität prüfen. Prozess-Optimierungen identifizieren. Schulungsbedarf ermitteln.

🎯 Jährlich

Strategische Bewertung des gesamten Governance-Frameworks. Abgleich mit regulatorischen Änderungen (EU AI Act). Roadmap für nächstes Jahr.

Ressourcen & Kontakt

Dieses Template ist Teil der Praxis-Toolbox von **kaffee-intelligenz.de** – dem Anlaufpunkt für pragmatische KI-Governance, die in der Realität funktioniert. Das KI-Logbuch bildet zusammen mit weiteren Templates wie dem AI Use Case Canvas, der Risikobewertungsmatrix und dem Prompt-Management-Framework ein geschlossenes Governance-System.

Weiterführende Ressourcen

📖 Buch: Kaffee.INTELLIGENZ

Das umfassende Handbuch für IT-Verantwortliche und AI-Governance-Teams. Von der Strategie über die Implementierung bis zum laufenden Betrieb – mit konkreten Templates, Checklisten und Fallbeispielen aus der deutschen Unternehmenslandschaft.

🌐 Online-Ressourcen

Auf **kaffee-intelligenz.de/** finden Sie die editierbare Version dieses Templates, ergänzende Video-Tutorials und eine Community für den Erfahrungsaustausch mit anderen Governance-Verantwortlichen.

Jetzt QR-Code scannen:

kaffee-intelligenz.de

📬 Kontakt

Philipp Diekmann
kaffee-intelligenz.de
Beratung · Workshops · Keynotes
Für KI-Governance, die nach Kaffee schmeckt – nicht nach Bürokratie.

☕ **Tipp:** Beginnen Sie mit Ihrem wichtigsten Use Case. Ein gut geführtes Logbuch für einen Use Case ist wertvoller als leere Templates für zehn.