



TOJO TECHNOLOGIES

ToJo Navigator

Modul: KI Governance

Decision Record

Anwendungsfall: Hosting-Entscheidung

Vollbericht mit Audit- und Umsetzungsanhang

Beispiel GmbH · Produktion & Maschinenbau · Mittel (50–249) · DE

Use Case: GenAI-Assistent zur Angebotserstellung im Vertrieb.

Enthält Management-Entscheidung, Freigabebedingungen, Audit-Anhang, Routinen, Nachweise, Kennzahlen und Methodik.

Entscheidungsreif mit Go-live-Auflagen

Empfehlung: **Public Cloud (mit Auflagen)**

Empfehlung entscheidungsreif — Produktivnahme erst nach Nachweis der Go-live-Auflagen

Datum: 22.09.2026 · Version 1 · erstellt: KI-Beauftragte, S. Musterfrau · **Vertraulich — nur zur internen Verwendung**

Strukturierte Entscheidungs- und Dokumentationsgrundlage auf Basis eines dreistufigen Bewertungsverfahrens · Methodik & Nachweise im Anhang

Inhalt (zum Springen anklicken)

1. [Management-Summary](#) S. 3 — Empfehlung & Begründung ([Begründung](#) S. 6)
2. [Auflagen & Freigabe](#) S. 11 — [Freigabebedingungen](#) S. 13 · [90-Tage-Plan](#) S. 15 · [Freigabe](#) S. 16
3. [Prüfung \(Anhang\)](#) S. 17 — [A3 Regulatorik](#) S. 17 · [A4 Machbarkeit](#) S. 22 · [A5 Nachweis](#) S. 23
4. [Betriebsroutinen \(A6\)](#) S. 32
5. [Routinen-Logbuch \(A6a\)](#) S. 38
6. [Kennzahlen & Methodik](#) S. 39 — [A7 Kennzahlen](#) S. 39 · [A9 Audit-Trail](#) S. 41 · [A10 Glossar](#) S. 41

Hinweis: Die Einträge sind anklickbare Sprungmarken. Die Seitenangaben werden aus dem fertigen Druck ermittelt und sind auf **eine Seite genau** — bei dicht gesetzten Tabellen kann ein Abschnitt eine Seite später beginnen.

Management-Summary

TOJO NAVIGATOR · MODUL: KI GOVERNANCE · ANWENDUNGSFALL: HOSTING-ENTSCHEIDUNG

Entscheidungsreif mit Go-live-Auflagen

Executive Dashboard

ENTSCHEIDUNGSSTATUS Entscheidungsreif mit Go-live-Auflagen	EMPFEHLUNG Public Cloud (mit Auflagen)
RISIKOKLASSE (EU AI ACT) Begrenztes Risiko	GO-LIVE nach Auflagen-Nachweis
GO-LIVE-NACHWEISE 10 offen · keine Blocker	VERANTWORTLICH KI-Beauftragte, S. Musterfrau
RESTAUFWAND (ORIENTIERUNG) überschaubar · 10 einmalige Nachweise	BELASTBARKEIT DER EMPFEHLUNG stark · Datenbasis vorläufig

Navigator-Version: 1.22.3

Erstellt: 22.09.2026

Freigegeben: ausstehend (siehe Auflagen)

Entscheidungs-Review: jährlich · Monitoring: quartalsweise

Gültig bis: bei Regulatorik-/Setup-Änderung

Dokumentstatus: Entscheidungsreif mit Go-live-Auflagen

Wissenschaftliche Grundlage

Dieses Decision Record basiert auf einem **wissenschaftlich entwickelten Bewertungsverfahren aus einer Dissertation** (Joswig 2026). Die Empfehlung wird **deterministisch anhand gewichteter Kriterien** berechnet; alle Ergebnisse sind **reproduzierbar und vollständig nachvollziehbar**. Keine Black Box, keine generative KI.

Prozessüberblick



Datensouveränität: EU-Region vor Go-live vertraglich absichern

Public Cloud bleibt die Empfehlung und ist mit Ihrer Vorgabe **EU-Datenresidenz** vereinbar: Die großen Anbieter (z. B. Microsoft Azure, AWS, Google Cloud) bieten EU- bzw. Deutschland-Regionen an. **Voraussetzung:** Der Anbieter garantiert die EU-Region **und** den AVV vertraglich — das ist eine **Auflage vor Go-live, kein Ausschlusskriterium**. Laut Ihrer Eingabe ist die EU-Region bereits vertraglich zugesichert; der Nachweis ist vor Go-live nachvollziehbar abzulegen. Die endgültige Freigabe erfordert eine **bewusste Geschäftsleitungs-Entscheidung nach Risikoabwägung**.

Ausgangslage: Mittel (50–249)-Unternehmen der Branche **Produktion & Maschinenbau**. Geplanter Anwendungsfall: „GenAI-Assistent zur Angebotserstellung im Vertrieb.“ (GenAI-Assistent). Verarbeitete Datenarten: **Personenbezogene Daten (DSGVO), Geschäftsgeheimnisse, Kundendaten (laut Compliance-Angabe)**. Aus diesen Angaben leiten sich die Auflagen, die regulatorische Einordnung und — bei personenbezogenen Daten oder Geschäftsgeheimnissen — die sicherheitsbezogene Betrachtung dieses Falls ab. **Ihr fallbezogenes Kernrisiko:** ein fehlerhafter oder erfundener Vorschlag, der ungeprüft übernommen wird — deshalb ist die menschliche Kontrolle der KI-Ausgaben (Routine 1/2) hier besonders wichtig.

Empfehlung: Public Cloud — starke Empfehlung (Abstand 0,64 zu Private Cloud)

Status: Entscheidungsreif mit Go-live-Auflagen — entscheidungsreif, aber noch NICHT produktiv freigegeben. Vor Go-live sind **10 Go-live-Auflage(n)** nachzuweisen; **2** weitere(r) Punkt(e) sind terminiert (später fällig) (siehe „Freigabebedingungen“; insgesamt 12). Der Sign-off bestätigt die Entscheidung, nicht die **technische Produktivfreigabe**. Zur Einordnung: Offene Auflagen sind überwiegend **einmalige Nachweise** (z. B. AVV ablegen, Verantwortliche/n benennen, Region bestätigen) — ein normaler Teil jeder KI-Einführung und **kein Mangel der Empfehlung selbst**.

Warum: Nach der Branchen-Standardbewertung (im Workshop an Ihren Fall zu schärfen): Public Cloud liegt bei den Kriterien vorn, die am schwersten wiegen: **Technische Passung** (Gewicht 30,6 %, Bewertung 5 von 5), **Organisatorische Passung** (Gewicht 21,4 %, Bewertung 5 von 5), **Wirtschaftlichkeit** (Gewicht 16,8 %, Bewertung 4 von 5). Den Abstand zu Private Cloud macht vor allem **Technische Passung** aus (5 gegenüber 4). Für einen GenAI-Assistenten zählen schnelle Bereitstellung und die Anbindung an Ihre bestehenden Systeme meist mehr als eigene Hardware.

Belastbarkeit: Die Empfehlung ist belastbar; Public Cloud liegt mit klarem Vorsprung vor Private Cloud (Abstand 0,64). **Vorbehalt: Für Ihre Branche (Produktion & Maschinenbau) liegt kein eigenes Startwert-Profil vor** — die Bewertungswerte sind branchenneutral. Die Aussage zur Belastbarkeit gilt für diese allgemeinen Startwerte, nicht für ein auf Ihren Sektor kalibriertes Modell. Der **Abstand** ist die Differenz der gewichteten Gesamtpunkte (jede Option wird je Kriterium mit 1–5 bewertet und mit den Gewichten aufsummiert). Skala: über 0,5 = stark · 0,2–0,5 = solide · 0,05–0,2 = knapp · unter 0,05 = keine eindeutige Empfehlung. **Grundlage der Einzelbewertungen:** Die je Kriterium vergebenen 1–5-Werte beruhen — soweit nicht im Workshop an Ihre konkrete Situation angepasst — auf **modellhaften Startwerten des Bewertungsmodells** (Ausgangsprofile je Option, keine erhobenen Kennzahlen — anders als die **Gewichte**, die aus der Expertenbefragung n=93 stammen); sie sind vor einer endgültigen Entscheidung zu prüfen.

Wirtschaftlichkeit: qualitatives Entscheidungskriterium; konkrete TCO-/Angebotsprüfung separat zu validieren.

Vor Go-live zu erledigen — die 5 dringendsten von 12 Auflagen

1. Sign-off der/des Verantwortlichen einholen (Geschäftsführung · vor Go-live)
2. Nachweis zur DE-/EU-Datenresidenz nachvollziehbar ablegen (EU) (IT-Leitung · vor Go-live)
3. Übermittlungsgrundlage für Drittländer festlegen und belegen (DSGVO Kapitel V) (DSB + Einkauf · vor Go-live)
4. Unterzeichneten AVV nachvollziehbar ablegen (DSB / Einkauf · vor Go-live)

Im Betrieb zu beobachten

- Verfügbarkeit — läuft die KI zuverlässig?
- Pflicht-Nachweise aktuell (Audit-Bereitschaft)
- keine ernststen KI-Vorfälle

5. Personenbezug & besondere Kategorien dokumentieren (DSB · vor Go-live)

Das sind die dringendsten. Die vollständige Liste aller **12** Freigabebedingungen mit Verantwortlichen und Fristen steht im Abschnitt „Freigabebedingungen“.

Die weiteren Abschnitte belegen die Empfehlung im Detail. Dieser Abschnitt dient als Entscheidungsgrundlage für die Geschäftsführung.

Kostenstruktur der Optionen — qualitativ (keine Euro-Beträge)

Public Cloud (empfohlen): Überwiegend laufende Kosten (nutzungsabhängig), kein nennenswerter Einmal-Invest; wächst mit der Nutzung.

Private Cloud: Höhere laufende Kosten als Public Cloud (nur für Sie reservierte Umgebung), meist geringer Einmal-Invest; mehr Kontrolle kostet einen Aufschlag.

AlaaS: Rein laufende Kosten (pro Nutzung bzw. Abo), am schnellsten startklar, kein Invest; abhängig vom Preismodell des Anbieters.

Hybrid: Geteilt: Einmal-Invest für den eigenen Teil plus laufende Kosten für den Cloud-Teil — die Höhe hängt davon ab, wo Sie den Schnitt legen.

On-Prem: Hoher Einmal-Invest vorab (Hardware/GPU), danach niedrigere laufende Kosten; lohnt bei planbarer Dauerlast.

Nur zur Orientierung — keine Euro-Beträge. Cloud/AlaaS verlagern Kosten von der Investition in den laufenden Betrieb; ein eigener Server bindet Kapital vorab. Die konkreten Zahlen liefert die separate TCO-/Angebotsprüfung im Workshop.

Abkürzungen in diesem Dokument — kurz erklärt

Reifegrad — Entwicklungsstand einer Betriebsroutine: 0 = nicht vorhanden, 1 = definiert, 2 = eingerichtet, 3 = nachgewiesen.

Freigabebedingung (Go-live-Auflage) — Auflage, die vor der Produktivnahme zu erfüllen und zu belegen ist.

Stopper — Kritischer Punkt, der eine Freigabe hart blockiert (z. B. kein AVV bei personenbezogenen Daten).

Sign-off — Förmliche Freigabe-Unterschrift der verantwortlichen Person.

DSGVO — Datenschutz-Grundverordnung der EU — regelt den Umgang mit personenbezogenen Daten.

DSB (Datenschutzbeauftragte/r) — Interne oder externe Person, die die Einhaltung des Datenschutzes überwacht.

AVV (Auftragsverarbeitungsvertrag) — Vertrag nach Art. 28 DSGVO, der regelt, wie ein Dienstleister personenbezogene Daten in Ihrem Auftrag verarbeitet.

DSFA (Datenschutz-Folgenabschätzung) — Prüfung nach Art. 35 DSGVO, ob eine Verarbeitung ein hohes Risiko für Betroffene birgt und welche Maßnahmen das senken.

VVT (Verzeichnis von Verarbeitungstätigkeiten) — Pflicht-Verzeichnis der Datenverarbeitungen nach Art. 30 DSGVO.

EU AI Act — EU-Verordnung zur Regulierung von KI; teilt Anwendungen in Risikoklassen (verboten, hoch, begrenzt, minimal) mit unterschiedlichen Pflichten ein.

High-Risk — Hochrisiko-KI im Sinne des AI Act (z. B. Personalauswahl, Kreditscoring) — strengere Pflichten.

AlaaS (AI as a Service) — Nutzung eines fertigen KI-Dienstes über eine Schnittstelle (API), ohne eigenes Modell zu betreiben.

NIS2 — EU-Richtlinie zur Cyber-Sicherheit für bestimmte Unternehmen und Sektoren.



**Rahmenbedingungen ·
Machbarkeit**
erfüllt



**Governance ·
Verantwortung**
bedingt erfüllt — Go-live-
Auflagen offen



**Entscheidungsbewertung
· Auswahl**
entscheidungsreif mit Go-live-
Auflagen

So nutzen Sie dieses Dokument

ABSCHNITT	WAS ES IST	WAS SIE DAMIT TUN
Teil 1 · Management Decision Record	Empfehlung, Belastbarkeit, Auflagen, Wirtschaftlichkeit (qualitativ), 90-Tage-Plan, Freigabe	dient als Entscheidungsgrundlage für die Geschäftsführung
Empfehlung & Begründung	Welche Option gewinnt und warum	als Begründung aufbewahren
Freigabebedingungen (Auflagen)	Was vor der Freigabe zu erfüllen ist	den Verantwortlichen zuordnen, abarbeiten
Nächste 90 Tage	Schritte mit Terminen	jeder Zeile eine/n Verantwortliche/n zuordnen
Teil 2 · Anhang (Audit & Umsetzung)	Detailprüfung Schritt 1–2, Routinen, Kennzahlen, Methodik, Audit-Trail, Glossar	für IT, Datenschutz und Prüfer — Nachweise ausfüllen und ablegen

Worum es geht

KI-ANWENDUNG	GenAI-Assistent zur Angebotserstellung im Vertrieb.
TYP	GenAI-Assistent
VERARBEITETE DATEN	Personenbezogene Daten (DSGVO), Geschäftsgeheimnisse, Kundendaten (laut Compliance-Angabe)
GEPRÜFTE OPTIONEN	Public Cloud, Private Cloud, On-Prem, Hybrid, AlaaS
WO DÜRFEN DIE DATEN LIEGEN?	EU/EWR

③ Empfehlung & Begründung

Die vollständige Detailprüfung von Schritt 1 (Machbarkeit) und Schritt 2 (Verantwortung & Nachweis) sowie die Routinen-Arbeitsvorlagen finden Sie im **Anhang**.

Empfehlung: **Public Cloud** — starke Empfehlung (Abstand 0,64 zu Private Cloud)

Vorläufige Empfehlung (Standard-Modus). Diese Bewertung beruht ausschließlich auf den **modellhaften Standardwerten des Bewertungsmodells**, nicht auf einer durchgehend eigenen Bewertung der Hosting-Optionen durch Ihr Haus — welche Einzelwerte Sie angepasst haben, weist die Bewertungsmatrix zellengenau aus. Der Abstand zwischen den Optionen ist daher eine **strukturelle Tendenz**, kein fallspezifisch gemessener Wert — bitte im Workshop bestätigen oder im Modus „Einfach“/„Experte“ eigene Einschätzungen ergänzen.

✓ Public Cloud		4,44
⚠ EU-Region erforderlich · laut Eingabe zugesichert · Nachweis offen		
Private Cloud		3,79
AlaaS		3,79
⚠ EU-Region erforderlich · laut Eingabe zugesichert · Nachweis offen		
Hybrid		3,58

On-Prem

3,04

Warum Public Cloud?

- sehr stark bei **Technische Passung** (Gewicht 30,6 %)
- sehr stark bei **Organisatorische Passung** (Gewicht 21,4 %)
- gut bei **Wirtschaftlichkeit** (Gewicht 16,8 %)

Der Abstand ist robust gegen einzelne Bewertungs-Unsicherheiten.

Bewertung über 8 gewichtete Kriterien; Balkenlänge = gewichteter Gesamtwert (max $\approx 5,0$). Verwendete Gewichtung: **Standardgewichtung des Bewertungsmodells** (Herleitung siehe Methodik-Anhang A2). Δ = EU-Region erforderlich (Status siehe Datensouveränität A3c). „**Nachweis offen**“ bedeutet: noch zu erbringen (vor Go-live), **kein bestätigter Mangel**. Bei **gleicher gerundeter Punktzahl** entscheidet der ungerundete Wert über die Reihenfolge (die Rangfolge im Balkendiagramm ist maßgeblich).

▼ Rechenweg & Bewertungsmatrix — so entsteht der Gesamtwert (5 Optionen × 8 Kriterien)

KRITERIUM	GEWICHT	PUBLIC CLOUD	PRIVATE CLOUD	AIAAS	HYBRID	ON-PREM
TECHNISCHE PASSUNG	0,3055	5 ^S	4 ^S	5 ^S	4 ^S	3 ^S
ORGANISATORISCHE PASSUNG	0,2137	5 ^E	4 ^S	4 ^S	3 ^S	3 ^S
WIRTSCHAFTLICHKEIT	0,1675	4 ^S	3 ^S	2 ^E	3 ^S	2 ^S
COMPLIANCE & SICHERHEIT	0,1102	3 ^S	4 ^S	2 ^S	4 ^S	5 ^S
KUNDENWIRKUNG & MARKTVERTRAUEN	0,0744	4 ^S	4 ^S	4 ^S	4 ^S	3 ^S
ZUKUNFTSOFFENHEIT	0,0588	5 ^S	4 ^S	5 ^S	4 ^S	3 ^S
PERSONAL & SKILLS	0,0393	4 ^S	3 ^S	5 ^S	3 ^S	2 ^S
RESTRISIKO	0,0305	3 ^S	4 ^S	2 ^S	4 ^S	4 ^S
Gewichteter Gesamtwert		4,44	3,79	3,79	3,58	3,04

Rechenweg: Gesamtwert = Summe aus (Rohwert 1–5 × Gewicht). Beispiel **Public Cloud**: $5 \times 0,3055 + 5 \times 0,2137 + 4 \times 0,1675 + 3 \times 0,1102 + 4 \times 0,0744 + 5 \times 0,0588 + 4 \times 0,0393 + 3 \times 0,0305 = \mathbf{4,44}$. (Gerechnet wird mit genau den hier gezeigten Gewichten; die Modellsomme beträgt rundungsbedingt 0,9999 statt 1,0000. Die Rechnung ist damit exakt nachvollziehbar.)

Herkunft der Rohwerte: ^E = von Ihnen gegenüber dem Startwert **angepasst** · ^S = unveränderter Branchen-Startwert des Bewertungsmodells. **2 von 40 Werten** (5 %) wurden von Ihnen gegenüber dem Startwert angepasst; die übrigen 38 sind unveränderte allgemeine Startwerte des Bewertungsmodells. **Für Ihre Branche (Produktion & Maschinenbau) liegt derzeit kein eigenes Startwert-Profil vor** — die Werte sind branchenneutral. Ein branchenspezifisches Profil ist bislang nur für Sektoren mit erhöhten Compliance-Anforderungen hinterlegt; für die übrigen werden bewusst keine Werte geschätzt. Die Startwerte sind **modellhafte Ausgangsprofile je Option**, keine erhobenen Kennzahlen; die **Gewichte** der Kriterien stammen dagegen aus der Expertenbefragung (n = 93) — siehe Anhang A2. Die Empfehlung ist so belastbar wie diese Werte und im Workshop mit Ihren Ist-Daten zu schärfen.

Wie stabil ist diese Empfehlung? Der Vorsprung ist robust (Abstand 0,64) — einzelne Bewertungsänderungen kippen die Empfehlung nicht. Jede Option wird je Kriterium mit **1–5** bewertet und gewichtet aufsummiert: **Public Cloud 4,44** vs. Private Cloud 3,79 — die **Differenz 0,64** ist der „Abstand“ (ab 0,5 stark · 0,2–0,5 solide · 0,05–0,2 knapp).

Andere Prioritäten testen? Im Schritt-3-Formular die **Gewichtung anpassen** und erneut auswerten — der Bericht weist die verwendete Gewichtung aus.

Sicherheitsbetrachtung — zweite Sicht auf die Empfehlung

Ihr Vorhaben ist **sicherheitssensibel** (personenbezogene Daten und Geschäftsgeheimnisse). Im Standardmodell wiegen **Compliance & Sicherheit (11,0 %)** und **Restrisiko (3,1 %)** zusammen nur **~14 %**, während technische und organisatorische Passung (zusammen ~52 %) die Empfehlung dominieren. Das ist methodisch korrekt, kann aber bei datensensiblen Vorhaben dazu führen, dass eine sicherere Option im Gesamtwert unterliegt. Das folgende **Alternativ-Ranking** zeigt die Reihenfolge, wenn Compliance/Sicherheit (28 %) und Restrisiko (12 %) deutlich schwerer gewichtet werden:

✓ Public Cloud		4,00
Private Cloud		3,85
Hybrid		3,71
On-Prem		3,53
AlaaS		3,25

Auch bei stark sicherheitsbetonter Gewichtung bleibt Public Cloud vorn — die Empfehlung ist damit auch aus Sicherheitsicht tragfähig. (Echte Compliance-Verstöße werden ohnehin bereits in Schritt 1/2 als **harte Stopper** abgefangen — nicht durch gute Werte in anderen Kriterien ausgleichbar —, unabhängig von dieser Gewichtung.)

Dies ist eine **Sensitivitäts-Illustration**, keine zweite offizielle Empfehlung. Ihre maßgebliche Gewichtung legen Sie im Schritt-3-Formular fest; die Standard-Empfehlung oben beruht auf der Forschungsgewichtung (n=93).

Was bedeutet das für Sie? — Interpretation

! Diese Interpretation wird **automatisch aus Ihren Bewertungsergebnissen erzeugt** (regelbasiert — **kein externes KI-Modell**, keine Übermittlung an KI-Dienste oder Dritte). Die Aussagen leiten sich direkt aus dem gewichteten Ranking ab; die Gegenmaßnahmen sind **Vorschläge zur Prüfung im Workshop**, keine Rechtsberatung.

Auf Basis der Standardgewichtung des Bewertungsmodells gewinnt **Public Cloud** mit klarem Vorsprung (4,44 zu 3,79 für Private Cloud). Über alle acht gewichteten Kriterien hinweg ergibt diese Option das beste Gesamtbild — nicht weil sie überall am besten ist, sondern weil sie dort stark ist, wo bei Ihrer Gewichtung das meiste Gewicht liegt.

Warum Public Cloud? Den Ausschlag geben vor allem: passt technisch gut zu Ihrer IT (zählt 30,6 %); passt zu Ihren Strukturen und Rollen (zählt 21,4 %); ist wirtschaftlich plausibel (qualitative Bewertung) (zählt 16,8 %). Genau diese Stärken fallen bei Ihrer Gewichtung am stärksten ins Gewicht.

Warum nicht Private Cloud? Public Cloud liegt vor allem bei **Technische Passung** und **Organisatorische Passung** vorn. Zwar ist Private Cloud bei **Compliance & Sicherheit** stärker, doch das wiegt bei Ihrer Gewichtung weniger und dreht das Ergebnis nicht.

Auffällig: Am schwächsten schneidet **On-Prem** ab — diese Option passt zu Ihrem Profil und Ihrer Gewichtung am wenigsten. Außerdem brauchen **Public Cloud** und **AlaaS** zwingend eine EU-Region/Datenresidenz, sonst entfallen sie.

Vorgeschlagene Gegenmaßnahmen

- **Datensouveränität:** Die empfohlene Option verarbeitet Daten außer Haus — EU-Region vertraglich festschreiben, Anbieter mit EU-Rechenzentrum + AVV wählen, ggf. einen Hybrid-Schnitt prüfen.
- **Compliance & Sicherheit (Bewertung 3/5):** Datenschutz-Folgenabschätzung (DSFA) und Auftragsverarbeitungsvertrag (AVV) aufsetzen, ein Audit-/Nachweiskonzept festlegen.
- **Restrisiko (Bewertung 3/5):** Restrisiken benennen, Rückfall-/Notfallplan (Routine 4) und laufendes Monitoring von Anfang an einrichten.
- **Worauf bei „Public Cloud“ besonders zu achten ist:** Ihre Daten verlassen das Haus — Anbieter, Region und Vertrag (Auftragsverarbeitung) müssen passen.

Was „Public Cloud“ konkret für Sie bedeutet

Was es ist: Ihre KI läuft beim Cloud-Anbieter (z. B. AWS, Microsoft Azure, Google). Sie mieten Rechenleistung, der Anbieter betreibt die Technik.

Für Sie: Schnell startklar, keine eigene Hardware, laufende statt investiver Kosten (konkrete Kosten separat zu validieren), wächst mit dem Bedarf.

Worauf achten: Ihre Daten verlassen das Haus — Anbieter, Region und Vertrag (Auftragsverarbeitung) müssen passen.

Anbieter-Bindung & Ausstieg (Exit). Bevor Sie sich festlegen, klären Sie den Ausstieg: **Datenexport** (in welchem Format bekommen Sie Ihre Daten und Modelle zurück?), **Portabilität** (läuft die Lösung nach einem Anbieterwechsel weiter?), **Kündigungs-/Löschfristen** und **proprietäre Formate/Schnittstellen**, die einen Wechsel teuer machen. Faustregel: Public Cloud / AlaaS binden am stärksten an den Anbieter, On-Prem am wenigsten (dafür tragen Sie Betrieb und Hardware selbst). Halten Sie Export- und Exit-Bedingungen **vertraglich** fest, bevor produktive Daten fließen.

Hosting-Optionen — Einordnung (Referenz)

Bewertet wurden in diesem Decision Record: Public Cloud, Private Cloud, On-Prem, Hybrid, AlaaS. Die folgenden Beschreibungen erläutern zusätzlich typische Hosting-Optionen zur Einordnung; **nicht bewertete Optionen sind nicht Teil der Empfehlung** (als „Referenz“ gekennzeichnet).

Public Cloud empfohlen

Was Sie brauchen: Ein Konto beim Cloud-Anbieter, eine eingerichtete Umgebung, Internetanbindung und einen Auftragsverarbeitungsvertrag (AVV) mit EU-Region. Kaum eigene Hardware.

Beispiel: Ihr KI-Assistent läuft in der Cloud (z. B. Microsoft Azure, Region Deutschland); Sie zahlen nach Nutzung, der Anbieter betreibt die Technik.

Wann sinnvoll: Schneller Start gewünscht, keine eigene Hardware/IT-Mannschaft, schwankende Last.

Private Cloud geprüft

Was Sie brauchen: Vertrag über eine nur für Sie reservierte Umgebung beim Anbieter; etwas mehr Konfiguration und Abstimmung als Public Cloud. Keine eigene Hardware im Haus.

Beispiel: Ein Anbieter stellt Ihnen eine abgeschottete, allein für Ihr Unternehmen reservierte Cloud-Instanz in einem EU-Rechenzentrum bereit.

Wann sinnvoll: Cloud-Komfort gewünscht, aber stärkere Datentrennung und Kontrolle als bei Public Cloud nötig.

On-Prem geprüft

Was Sie brauchen: Einen eigenen Server im Haus, bei KI meist mit Grafikkarte (GPU); einen abgesicherten Raum (Strom, Kühlung); IT-Personal für Betrieb und Updates; ein Backup- und Notfallkonzept.

Beispiel: Sie stellen einen GPU-Server in Ihren Serverraum und betreiben darauf ein offenes KI-Modell (z. B. über Ollama). Die Daten verlassen nie das Haus.

Wann sinnvoll: Strenge Datenschutz-/Geheimhaltungsanforderungen, vorhandene IT-Mannschaft, planbare Dauerlast.

Hybrid geprüft

Was Sie brauchen: Eine Kombination: eigene Umgebung für die sensiblen Teile UND einen Cloud-/Anbieter-Zugang für den Rest — plus eine klar definierte Schnittstelle und Zuständigkeit dazwischen.

Beispiel: Sensible Kundendaten werden im Haus verarbeitet, die rechenintensive Modellauswertung läuft in der EU-Cloud; eine festgelegte Schnittstelle verbindet beides.

Wann sinnvoll: Ein Teil der Daten muss im Haus bleiben, anderes soll aber von der Cloud-Skalierung profitieren.

AlaaS geprüft

Was Sie brauchen: Nur einen Vertrag und einen Zugang (API-Schlüssel) zum fertigen KI-Dienst; keine eigene Hardware, kein eigener Betrieb. Datenschutzvertrag (AVV) und Datenfluss klären.

Beispiel: Ihre Software ruft über eine Schnittstelle einen fertigen KI-Dienst auf; Sie betreiben selbst weder Modell noch Server.

Wann sinnvoll: Schnellster Start, kein Eigenaufwand, keine eigene KI-Mannschaft — Abhängigkeit vom Anbieter wird akzeptiert.

Wirtschaftlichkeit (qualitativ — keine TCO-Zahlen in dieser Erstbewertung)

Die Wirtschaftlichkeit ist in Schritt 3 (Entscheidungsbewertung) als **qualitatives Bewertungskriterium** in die Empfehlung eingeflossen (siehe Begründung oben). **TCO-/Angebotsprüfung: offen / separat zu validieren.**

Warum hier keine Euro-Beträge? Eine belastbare Kostenrechnung braucht konkrete Anbieter-Angebote und Ihre Ist-Kosten (Personal, Infrastruktur, Lizenzen) — beides entsteht erst im Workshop. Eine an dieser Stelle erfundene Zahl wäre **schlechter als keine**. Als Orientierung dient die folgende **relative Kosten-Rangfolge** (ohne Beträge); die konkreten Zahlen liefert die TCO-/Angebotsprüfung.

OPTION	ANFANGSINVESTITION	LAUFENDE KOSTEN	ANBIETERBINDUNG
★ PUBLIC CLOUD	niedrig	mittel · nutzungsabhängig	hoch
PRIVATE CLOUD	niedrig–mittel	mittel–hoch	mittel
AIAAS	sehr niedrig	mittel–hoch · Abo/Nutzung	hoch
HYBRID	mittel	mittel	mittel
ON-PREM	hoch	niedrig	niedrig

Relative Einordnung (niedrig / mittel / hoch), **keine Beträge**. ★ = empfohlene Option. „Anbieterbindung“ = wie aufwendig ein späterer Wechsel wäre (Details unter „Anbieter-Bindung & Ausstieg“ bei der Empfehlung). Diese Rangfolge ist ein **Strukturvergleich**, kein Angebot — die tatsächlichen Kosten hängen von Nutzungsvolumen, Anbieter und Vertrag ab.

Eine detaillierte TCO-/Angebotsprüfung ist **nicht Bestandteil dieser Erstbewertung**. Vor einer Beschaffungs- oder Umsetzungsentscheidung sollten konkrete Anbieterangebote, interne Aufwände, Integrationskosten, Security-/Compliance-Aufwände, Support-Level und laufende Betriebskosten separat validiert werden. Ein dediziertes Modul „TCO & Beschaffungsvalidierung“ kann dies später ergänzen.

Risiko-Matrix (qualitative Einordnung aus Ihren Angaben)

RESTRISIKO NACH MASSNAHME*						
RISIKO	EINTRITT	AUSWIRKUNG	STATUS	VERANTWORTLICH	MASSNAHME	
■ Offene Go-live-Auflagen ↳ ausgelöst durch: 10 noch offene Auflage(n) aus der Freigabe-Prüfung (Abschnitt ②)	sicher	mittel	gering (erwartet)	offen	KI-Beauftragte, S. Musterfrau	10 Auflage(n) vor Go-live nachweisen
■ Datensouveränität / Drittlandzugriff ↳ ausgelöst durch: Datenresidenz-/Souveränitäts-Anforderung (Schritt 1) + externe Hosting-Empfehlung	mittel	hoch	gering	Auflage	DSB / IT	EU-Region + AVV vertraglich zusichern und nachweisen
■ Security-Baseline nicht nachgewiesen ↳ ausgelöst durch: externes Hosting + Security-Nachweise nicht als „geprüft“ bestätigt (Anbieter-Block)	mittel	hoch	gering (erwartet)	offen	IT / Security	18-Punkte-Security-Baseline ablegen und prüfen
■ Manipulierte Eingaben (Prompt-Injection) ↳ ausgelöst durch: Anwendungsfall als GenAI-/Sprach-Anwendung erkannt (Feld „KI-Anwendung“ bzw. Anwendungsfall-Typ)	mittel	hoch	mittel	laufend	IT / Security	Ein- und Ausgaben härten (Filter/Trennung von Anweisung und Daten); Injection-Tests vor Go-live und bei Änderungen
■ Fehlerhafte oder erfundene KI-Ausgaben (Halluzination) ↳ ausgelöst durch: Anwendungsfall als GenAI-/Sprach-Anwendung erkannt (Feld „KI-Anwendung“ bzw. Anwendungsfall-Typ)	mittel	mittel	mittel	laufend	Fachbereich	Stichproben-/Qualitätskontrolle; kritische Ausgaben menschlich prüfen (Routine 1/2)

RISIKO	EINTRITT	AUSWIRKUNG	RESTRISIKO NACH MASSNAHME*	STATUS	VERANTWORTLICH	MASSNAHME
Nachlassende Ausgabequalität über die Zeit (Modell-Drift) ↳ ausgelöst durch: Anwendungsfall als GenAI-/Sprach-Anwendung erkannt (Feld „KI-Anwendung“ bzw. Anwendungsfall-Typ)	mittel	mittel	mittel	laufend	Fachbereich / IT	Qualität regelmäßig gegen feste Referenz-Testfälle prüfen (Routine 2); als Kennzahl überwachen
Anbieter-Ausfall / Nichtverfügbarkeit ↳ ausgelöst durch: externe Hosting-Empfehlung (Betrieb beim Anbieter)	niedrig	mittel	gering	vertraglich	IT	SLA vereinbaren; Fallback-/Notfallprozess definieren (Routine 4)
Datenabfluss in das Training des Anbieter-Modells ↳ ausgelöst durch: personenbezogene Daten (Daten & Compliance) + externes Hosting; Trainingsausschluss „ja“ → entschärft	niedrig	hoch	gering	vertraglich ausgeschlossen	DSB / IT	Trainings-Ausschluss (Zero-Retention) vertraglich sichern und nachweisen
Anbieter-Abhängigkeit (Vendor-Lock-in) ↳ ausgelöst durch: empfohlene Option „Public Cloud“ hat hohe Anbieterbindung (Kostenmodell)	mittel	mittel	mittel	beobachten	IT / Einkauf	Exit-Strategie: Datenexport, Portabilität, Kündigungsfristen vertraglich (siehe Lock-in-Kasten)

Sortiert nach Schweregrad (höchstes Risiko zuerst): erst Governance-/Freigabe-Auflagen, dann die KI-Betriebsrisiken. Die Zeile „**ausgelöst durch**“ zeigt je Risiko, welche Ihrer Eingaben es erzeugt hat — die Matrix ist eine Ableitung aus dem Formular, keine separate Eingabe. * **Restrisiko** = verbleibende Bewertung **nach** Umsetzung der genannten Maßnahme. Qualitative Einordnung aus Ihren Angaben — keine vollständige Risikoanalyse; unternehmensspezifische Risiken (z. B. betriebliche Abhängigkeiten) sind gesondert zu bewerten.

Status: Entscheidungsreif mit Go-live-Auflagen — die KI ist derzeit **NICHT produktiv freigegeben**. Die Produktivnahme ist erst nach Nachweis der unten gelisteten Go-live-Auflagen zulässig; der Sign-off bestätigt die Entscheidung, nicht die Produktivnahme.

Freigabebedingungen (Auflagen)

Die Empfehlung ist **entscheidungsreif**. Die **Produktivnahme** ist erst zulässig, wenn die folgenden Go-live-Auflagen nachgewiesen sind. Status zum Stand dieses Dokuments:

Empfohlene Reihenfolge (kritischer Pfad) — womit anfangen? Nicht alle Auflagen sind gleich dringlich; diese Reihenfolge vermeidet Nacharbeit (z. B. muss der Anbieter-/AVV-Rahmen stehen, bevor Security-Nachweise Sinn ergeben):

1 · Rechtliche & vertragliche Grundlagen zuerst (vor Go-live zwingend — Voraussetzung für die übrigen Nachweise)

1. Nachweis zur DE-/EU-Datenresidenz nachvollziehbar ablegen (EU) (IT-Leitung · vor Go-live)
2. Übermittlungsgrundlage für Drittländer festlegen und belegen (DSGVO Kapitel V) (DSB + Einkauf · vor Go-live)
3. Unterzeichneten AVV nachvollziehbar ablegen (DSB / Einkauf · vor Go-live)
4. Personenbezug & besondere Kategorien dokumentieren (DSB · vor Go-live)
5. DSFA-Relevanz bewerten (DSB · vor Go-live)
6. Informationspflichten und Betroffenenrechte anpassen (DSGVO Art. 13/14) (DSB · vor Go-live)
7. Vertraulichkeit & Geheimnisschutz prüfen (IT + Fachbereich · vor Go-live)

2 · Verantwortlichkeiten benennen (ohne benannte Person keine Freigabe)

8. Sign-off der/des Verantwortlichen einholen (Geschäftsführung · vor Go-live)
9. Risiko-Check vor Produktivnahme abschließen (IT + Fachbereich · vor Go-live)

3 · Security- & sonstige Nachweise ablegen

10. Security-Baseline-Nachweise ablegen und prüfen (IT-Leitung / Security · vor Go-live)

Geschätzter Gesamtaufwand: 42 Arbeitspakete — die konkreten Detailschritte der 10 offenen Auflagen (davon 27 gering, 15 mittel), über die 90-Tage-Phasen verteilt; überwiegend einmalige Nachweise, kein Daueraufwand. Feinschätzung im Workshop.

#	FREIGABEBEDINGUNG	WARUM	VERANTWORTLICH	FRIST	ERLEDIGT	STATUS
1	Sign-off der/des Verantwortlichen einholen	Accountable benannt (KI-Beauftragte, S. Musterfrau) — formale Freigabe ausstehend	Geschäftsführung	vor Go-live	☐	offen
2	Nachweis zur DE-/EU-Datenresidenz nachvollziehbar ablegen (EU)	Verarbeitungsregion (Belegheitsort) vertraglich gesichert — Nachweis ablegen; die Übermittlungsgrundlage nach Kapitel V wird gesondert geführt	IT-Leitung	vor Go-live	☐	offen
3	Übermittlungsgrundlage für Drittländer festlegen und belegen (DSGVO Kapitel V)	Externe Verarbeitung personenbezogener Daten — die Verarbeitungsregion allein ist keine Übermittlungsgrundlage	DSB + Einkauf	vor Go-live	☐	offen
4	Unterzeichneten AVV nachvollziehbar ablegen	DSGVO Art. 28 — AVV abgeschlossen, Nachweis ablegen	DSB / Einkauf	vor Go-live	☐	offen
5	Personenbezug & besondere Kategorien dokumentieren	DSGVO Art. 9	DSB	vor Go-live	☐	offen
6	DSFA-Relevanz bewerten	DSGVO Art. 35	DSB	vor Go-live	☐	offen

#	FREIGABEBEDINGUNG	WARUM	VERANTWORTLICH	FRIST	ERLEDIGT	STATUS
7	Informationspflichten und Betroffenenrechte anpassen (DSGVO Art. 13/14)	Neue Verarbeitung — Datenschutzhinweise und Auskunftsprozess müssen sie abbilden	DSB	vor Go-live	☐	offen
8	Risiko-Check vor Produktivnahme abschließen	Betriebsverantwortung	IT + Fachbereich	vor Go-live	☐	offen
9	Monitoring- & Incident-Prozess festlegen	Betriebssicherheit	IT-Leitung	Tag 30	☐	ausstehend
10	NIS2-Betroffenheit feststellen und, falls zutreffend, Pflichten umsetzen	Sektor Produktion & Maschinenbau fällt dem Grunde nach unter Anhang II (verarbeitendes Gewerbe) — nur für bestimmte Erzeugnisse, u. a. Medizinprodukte, Elektro, Maschinenbau, Kraftfahrzeuge	Geschäftsführung + IT-Leitung	Tag 30	☐	ausstehend
11	Vertraulichkeit & Geheimnisschutz prüfen	Kundendaten / Geschäftsgeheimnisse	IT + Fachbereich	vor Go-live	☐	offen
12	Security-Baseline-Nachweise ablegen und prüfen	Informationssicherheit / Auditfähigkeit (Nachweise vor Go-live)	IT-Leitung / Security	vor Go-live	☐	offen

Setzen Sie das **Häkchen „Erledigt“**, sobald eine Bedingung nachgewiesen ist — **oder erledigen Sie alle Einzelschritte** unten, dann wird die Bedingung automatisch . Legende:  **erfüllt** — nachgewiesen ·  **offen** — vor Go-live zu erledigen, **blockiert die Produktivnahme** ·  **nicht erfüllt** — Produktivnahme nicht zulässig ·  **ausstehend** — verbindlich terminiert, kurz nach Produktivnahme einzurichten/nachzuweisen (keine reine Beobachtung; rechtlich/Go-live-relevante Pflichten sind als „offen“ geführt).

Die **konkreten Einzelschritte je Bedingung** — mit Abnahmekriterium, grobem Aufwand und den ausfüllbaren Nachweis-Vorlagen — stehen im Anhang unter **A5b**. Dieser Abschnitt bleibt damit die Entscheidungsgrundlage; die Arbeitsvorlagen für DSB und IT liegen hinten.

Ihre nächsten 90 Tage

Warum diese Zeitfenster? Die Schritte sind nach **Dringlichkeit und logischer Reihenfolge** gestaffelt — von „blockiert die Produktivnahme“ bis „laufender Betrieb“:

Sofort (0–14 Tage): was die Produktivnahme blockiert oder sofort zu klären ist (Freigabe/Sign-off, kritische Security-Nachweise, Compliance-Stopper). · **Bis Tag 30:** offene Pflicht-Punkte und Auflagen vor dem Go-live schließen (Machbarkeits-/Governance-Lücken, Datenresidenz/Verträge). · **Bis Tag 60:** Betrieb aufsetzen (Routinen vervollständigen, KPI-Baseline etablieren, Datenquellen anbinden). · **Bis Tag 90:** ersten Review-Zyklus fahren (Quartals-Scorecard) und den Decision Record fortschreiben.

Die Fristen sind **Empfehlungen**, keine harten Termine — passen Sie sie an Ihre Situation an. Ein Schritt steht in dem Zeitfenster, das seiner Funktion entspricht (z. B. Freigabe-Stopper „sofort“, Kennzahlen-Aufbau „Tag 60“).

Technische Umsetzung (Track für die IT). Neben den organisatorischen Schritten gehören in die Umsetzung: **Sizing / Proof of Concept** — die gewählte Option an einem echten Anwendungsfall testen (Last, Antwortzeiten, Kosten), bevor produktiv geschaltet wird; **Integration & Schnittstellen (API)** — Anbindung an Ihre Systeme, Authentifizierung und Datenflüsse festlegen; **Datensicherung & Wiederanlauf** — Backup-Konzept mit Zielwerten für Wiederherstellzeit (RTO) und tolerierbaren Datenverlust (RPO) plus getestetem Fallback. Diese Punkte plant die IT parallel zu den Auflagen; sie sind kein Freigabe-Stopper, aber vor dem produktiven Vollbetrieb abzuschließen.

ERLEDIGT	SCHRITT	VERANTWORTLICH	FERTIG, WENN ...	AUFWAND
Sofort (0–14 Tage)				
☒	↑ <u>Auflage</u> Sign-off der/des Verantwortlichen einholen (Freigabe dokumentieren)	Geschäftsführung	Sign-off im Freigabe-Feld erfasst	gering
☒	↑ <u>Auflage</u> Security-Baseline-Nachweise ablegen und prüfen	IT-Leitung / Security	kritische Security-Nachweise abgelegt und geprüft	mittel
Bis Tag 30				
☒	↑ <u>Auflage</u> Souveränitäts-/Compliance-Auflagen der gewählten Option umsetzen	IT + DSB	Region/Vertragslage vertraglich nachgewiesen	mittel
Bis Tag 60				
☐	KPI-Baseline (Starter-5) etablieren, Datenquellen anbinden	Controlling + IT	Starter-5 mit ersten Ist-Werten befüllt	gering
Bis Tag 90				
☐	Erste Review-Runde (Scorecard) fahren, Decision Record fortschreiben	Geschäftsführung	Erste Quartals-Review dokumentiert	gering

Aufwand grob geschätzt (gering ≈ Stunden, mittel ≈ Tage). Personen aus Ihren Angaben/Schritt 2 übernommen; in kleinen Firmen bündelt die Geschäftsführung mehrere Rollen. Häkchen setzen, wenn erledigt — erledigte Schritte werden **durchgestrichen, gezählt** und automatisch gespeichert (auch in der Decision-Record-Datei). Aufgaben mit „↑ **Auflage**“ sind zugleich **Freigabebedingungen** — diese haken Sie **oben bei den Freigabebedingungen** ab (eine Quelle, kein doppeltes Abhaken) — der Verweis springt dorthin und hebt die Bedingung hervor. Die **übrigen Schritte mit Kästchen** sind reine Umsetzungs-/Betriebsaufgaben (z. B. Kennzahlen, Review), die es **nur hier** gibt — diese haken Sie hier ab.

Freigabe

Zwei Unterschriften — getrennte Verantwortung: Die **Geschäftsführung** zeichnet die **Entscheidung** (Wahl der Hosting-Option, wirtschaftliche/strategische Verantwortung). **IT/DSB/CSO** zeichnen die **Nachweise & Auflagen** (Security-Baseline, AVV, Datenresidenz, DSFA-Relevanz — die Fachprüfung). Die **Produktivnahme** wird erst freigegeben, wenn **beide** vorliegen. So bestätigt die Geschäftsführung keine Sicherheits-/Datenschutzaussage, für die sie fachlich nicht einsteht.

Verantwortliche/r für die KI-Anwendung (Accountable): _____ — die Person, die für den verantwortungsvollen Betrieb geradesteht.

ROLLE	BESTÄTIGT	NAME	DATUM
Geschäftsführung	Entscheidung (Hosting-Wahl)	_____	_____
IT / DSB / CSO	Nachweise & Auflagen (Fachprüfung)	_____	_____

ROLLE	BESTÄTIGT	NAME	DATUM
Berater	Erstellung	KI-Beauftragte, S. Musterfrau	22.09.2026

Hinweis: Die IT/DSB/CSO-Unterschrift wird an den geprüften Stand gebunden. Bitte **zuletzt** unterschreiben — nachdem alle Auflagen und Angaben stehen.

Grenze der digitalen Unterschrift: Die Unterschriften und das Vier-Augen-Prinzip beruhen auf den eingetragenen Namen sowie — bei aktiver Verschlüsselung — auf dateigebundenen Signaturen. Sie machen nachträgliche Änderungen **erkennbar** (tamper-evident), erzwingen aber keine **authentifizierte Personen-Identität**: Wer Zugriff hat, könnte einen Namen frei eintragen. Eine server-geprüfte Identität, die das ausschließt, ist ein geplanter Ausbau — bis dahin ersetzt die Unterschrift hier ein internes Freigabe-Protokoll, keine rechtsverbindliche eID.

Anhang · Audit & Umsetzung

Dieser Anhang richtet sich an IT, Datenschutz, Compliance und Prüfer. Er dokumentiert die Methodik, die zugrunde liegenden Annahmen, die regulatorischen Bezüge, die Nachweise sowie die operativen Routinen zur Umsetzung der empfohlenen KI-Hosting-Entscheidung. Er ergänzt den vorangestellten Management Decision Record und richtet sich primär an IT, Datenschutz, Compliance und Prüfer.

A1

Verfahren & Bewertungslogik

Strukturiertes 3-Schritte-Verfahren (Machbarkeit → Verantwortung → Auswahl) aus einer Dissertation zur KI-Governance im Mittelstand (Joswig, 2026). Schritt 1 und 2 arbeiten mit Schwellenwerten (eine nicht erfüllte Pflicht-Voraussetzung stellt die Entscheidung zurück); Schritt 3 vergleicht die Optionen über eine gewichtete additive Bewertung (AHP). Wirtschaftlichkeit fließt als qualitatives Kriterium ein; eine detaillierte TCO-/Angebotsprüfung ist separat zu validieren.

A2

Gewichtung & Datenbasis

Die Gewichte der 8 Auswahl-Kriterien stammen aus einer Expertenbefragung (n = 93) nach dem Analytic-Hierarchy-Process (AHP). Die Gewichte bilden einen **globalen Vektor** (Modellsumme 0,9999, rundungsbedingt) und sind **nicht branchenspezifisch** — branchenspezifisch sind allein die **Roh-Startwerte** der Optionen (1–5), die je Sektor voreingestellt sind. Erhebungsmethode, Stichprobenzusammensetzung und die Konsistenzprüfung der paarweisen Vergleiche (AHP Consistency Ratio) sind in der zugrunde liegenden Dissertation (Joswig 2026) dokumentiert. **Es handelt sich um eine eigene Erhebung, nicht um eine externe Validierung der Gewichte.** Zwei zugehörige Beiträge sind veröffentlicht (Journal of Next Generation Research 5.0): doi.org/10.70792/jngr5.0.v1i2.89 und doi.org/10.70792/jngr5.0.v1i3.99. In dieser Auswertung verwendete Gewichtung: **Forschungsgewichte (Dissertation, n = 93)**. Abweichungen von den Standardwerten werden hier und in Schritt 3 ausgewiesen.

A3

Regulatorischer Rahmen

Einschlägig laut Angaben: EU AI Act (Klasse limited), DSGVO, NIS2 (sofern zutreffend). Sektor: Produktion & Maschinenbau. Die maßgeblichen Pflichten ergeben sich aus Schritt 1 (Sektor- & Datenschutz-Fragen) und den Nachweisen aus Schritt 2.

REGELWERK	EINSCHLÄGIGE ARTIKEL (ORIENTIERUNG)
EU AI Act (Klasse limited)	Art. 50 (Transparenzpflichten); allgemeine Betreibersorgfalt
DSGVO	Art. 6 (Rechtsgrundlage), Art. 30 (VVT), Art. 32 (Sicherheit), Art. 13/14 (Informationspflichten), Art. 28 (Auftragsverarbeitung), Art. 44–49 (Übermittlung in Drittländer: Art. 45/46/49 + Transfer Impact Assessment)
NIS2 / Sicherheit	Ihr Sektor Produktion & Maschinenbau fällt dem Grunde nach unter Anhang II (verarbeitendes Gewerbe) (nur für bestimmte Erzeugnisse, u. a. Medizinprodukte, Elektro, Maschinenbau, Kraftfahrzeuge); die Größenklasse Mittel (50–249) spricht ebenfalls dafür. Die Betroffenheit ist damit nicht feststellt, sondern zu prüfen — siehe eigene Freigabebedingung. Maßgeblich ist das BSIG in der Fassung des NIS2-Umsetzungsgesetzes (unionsrechtlich Art. 21 Risikomanagement, Art. 23 Meldepflichten). Meldekette bei erheblichen Sicherheitsvorfällen: Frühwarnung 24 Stunden · Meldung 72 Stunden · Abschlussbericht ein Monat , dazu Registrierung beim BSI.

Artikelangaben dienen der Orientierung und ersetzen keine rechtliche Prüfung.

AI-Act-Einordnung: Limited Risk auf Basis der Angaben. Kein High-Risk-Befund aus den vorliegenden Eingaben. Einzelne Kontrollpunkte in der Matrix unten werden **vorsorglich als Governance-Nachweise** verwendet und bedeuten **nicht**, dass das System als High-Risk eingestuft wurde. Bei Änderung des Use Cases,

automatischer Entscheidung mit erheblicher Personen-/Kundenwirkung oder Einsatz in regulierten Hochrisikobereichen ist die Einordnung erneut zu prüfen.

A3a

Control-/Evidence-Matrix (Auflage → Regulatorik → Nachweis)

EVIDENZ	AUFLAGE / KONTROLLE	REGULATORIK-BEZUG	NACHWEIS (ARTEFAKT)	VERANTWORTLICH	FRIST	STATUS
E-01	Sign-off der/des Verantwortlichen einholen	Governance / Rechenschaft (DSGVO Art. 5 Abs. 2) · ISO/IEC 27001 A.5.2 · bei Hochrisiko zusätzlich EU AI Act Art. 26 (Betreiberpflichten)	Sign-off im Freigabe-Feld erfasst	Geschäftsführung	vor Go-live	offen
E-02	Nachweis zur DE-/EU-Datenresidenz nachvollziehbar ablegen (EU)	DSGVO Art. 44–49 (Übermittlung in Drittländer) · Art. 30 Abs. 1 lit. e	Subprozessoren geprüft & dokumentiert	IT-Leitung	vor Go-live	offen
E-03	Übermittlungsgrundlage für Drittländer festlegen und belegen (DSGVO Kapitel V)	DSGVO Art. 44–49 (Übermittlung in Drittländer) · Art. 30 Abs. 1 lit. e	Übermittlungsgrundlage (Angemessenheitsbeschluss/SCC) + Transfer Impact Assessment abgelegt	DSB + Einkauf	vor Go-live	offen
E-04	Unterzeichneten AVV nachvollziehbar ablegen	DSGVO Art. 28 (Auftragsverarbeitung)	AVV auch für weitere Dienstleister vorhanden/geprüft	DSB / Einkauf	vor Go-live	offen
E-05	Personenbezug & besondere Kategorien dokumentieren	DSGVO Art. 9 (besondere Kategorien) · Art. 30 (VVT)	VVT aktualisiert	DSB	vor Go-live	offen
E-06	DSFA-Relevanz bewerten	DSGVO Art. 35 (Datenschutz-Folgenabschätzung)	DSB-Stellungnahme abgelegt	DSB	vor Go-live	offen

EVIDENZ	AUFLAGE / KONTROLLE	REGULATORIK-BEZUG	NACHWEIS (ARTEFAKT)	VERANTWORTLICH	FRIST	STATUS
E-07	Informationspflichten und Betroffenenrechte anpassen (DSGVO Art. 13/14)	DSGVO Art. 13/14 (Informationspflichten) · Art. 15, 17, 21 (Betroffenenrechte)	Aktualisierte Datenschutzhinweise + erweiterter Prozess für Betroffenenanfragen	DSB	vor Go-live	offen
E-08	Risiko-Check vor Produktivnahme abschließen	DSGVO Art. 32 (Sicherheit) · gute Praxis (bei Hochrisiko: EU AI Act Art. 9/14)	Protokoll abgelegt	IT + Fachbereich	vor Go-live	offen
E-09	Monitoring- & Incident-Prozess festlegen	DSGVO Art. 33 (Meldepflicht) · NIS2 Art. 23 (sofern NIS2-pflichtig) · EU AI Act Art. 72/73 (bei Hochrisiko)	Review-Termin steht	IT-Leitung	Tag 30	ausstehend
E-10	NIS2-Betroffenheit feststellen und, falls zutreffend, Pflichten umsetzen	BSiG i. d. F. des NIS2-Umsetzungsgesetzes · unionsrechtlich Art. 21, 23 der Richtlinie (EU) 2022/2555	Dokumentierte Betroffenheitsprüfung; falls betroffen: Registrierungsnachweis und Meldeprozess mit Fristen	Geschäftsführung + IT-Leitung	Tag 30	ausstehend
E-11	Vertraulichkeit & Geheimnisschutz prüfen	DSGVO Art. 32 (Sicherheit) · GeschGehG	Datenfluss geprüft, ggf. anonymisiert	IT + Fachbereich	vor Go-live	offen
E-12	Security-Baseline-Nachweise ablegen und prüfen	DSGVO Art. 32 · NIS2 Art. 21 · ISO/IEC 27001	Nachweis abgelegt	IT-Leitung / Security	vor Go-live	offen

Die Evidenz-IDs (E-01 ...) verknüpfen jede Auflage mit ihrem regulatorischen Bezug und dem abzulegenden Nachweis. Der Erfüllungsstand wird über die Häkchen in Abschnitt ② „Auflagen & Freigabe“ gepflegt; laufende Nachweise dokumentiert das Routinen-Logbuch (A6a). Artikelangaben dienen der Orientierung und sind keine Rechtsberatung.

A3b

Anbieter- & Security-Prüfung

Bei Public Cloud / AlaaS verlassen Daten Ihr Haus. Erfasste Angaben (Nachweise sind gesondert abzulegen). „Nein“ bei AVV/Residenz/Training ist ein **harter Stopper**; „unklar“/„in Prüfung“/„teilweise/offen“ werden als **Auflage** in den Freigabebedingungen geführt.

Anbieter	Microsoft Azure
----------	-----------------

Dienst / Modell	Azure OpenAI Service
Hosting-Region	EU (Frankfurt / Schweden)
DE-/EU-Region vertraglich	ja
Auftragsverarbeitung (AVV)	ja, abgeschlossen
Subprozessoren bekannt	ja
Supportzugriffe außerhalb EU/EWR	✓ nein — kein Drittlandzugriff
Training mit Ihren/Kundendaten ausgeschlossen	ja
Lösch-/Rückgabekonzept	ja
Security-Baseline (Gesamt)	Go-live-Auflage offen — Kontrollpunkt(e) nur mit Auflage erfüllt

Security-Baseline — Kontrollpunkte. Je Punkt **einzeln im Navigator bewertet** (★ = kritisch). Zwei Ebenen: **Bewertung** aus der Eingabe, **Nachweis** erst nach Ablage/Prüfung. Alle Bewertungen sind zunächst **Selbstauskunft** und gelten erst dann als geprüft, wenn der jeweilige Nachweis abgelegt und von der Fachprüfung (IT/DSB/CSO) bestätigt wurde.

KONTROLLPUNKT	BEWERTUNG	NACHWEIS	ABLAGEORT	NACHWEIS / QUELLE
★ MFA für Admin-/alle Zugänge	erfüllt laut Eingabe	✓ Nachweis geprüft (laut Eingabe)	Wiki/Security-Baseline	Policy / Screenshot / Anbieter-Doku
★ Rollen-/Rechtekonzept (Least Privilege)	erfüllt laut Eingabe	✓ Nachweis geprüft (laut Eingabe)	—	Rechtekonzept-Dokument
Sichere Admin-/Fernzugänge (schlüsselbasiert, kein Passwort-Login)	erfüllt laut Eingabe	✓ Nachweis geprüft (laut Eingabe)	—	Zugangs-/SSH-Konfiguration
★ API-Key-Speicherung (Secret-Store)	erfüllt laut Eingabe	✓ Nachweis geprüft (laut Eingabe)	—	Konfiguration Secret-Store
API-Key-Rotation	erfüllt mit Auflage	Nachweis offen	—	Rotation-Policy
★ Verschlüsselung in Transit (TLS)	erfüllt laut Eingabe	✓ Nachweis geprüft (laut Eingabe)	SharePoint/IT-Security	Anbieter-/Konfig-Nachweis
★ Verschlüsselung at Rest	erfüllt laut Eingabe	Nachweis abgelegt	—	Anbieter-/Konfig-Nachweis
★ Logging / Audit-Logs	erfüllt laut Eingabe	Nachweis abgelegt	DMS/Audit	Logging-Konfiguration
Monitoring / Alerting	erfüllt laut Eingabe	Nachweis abgelegt	—	Monitoring-Konfiguration
Patch-/Update-Management (Betriebssystem & Abhängigkeiten)	erfüllt mit Auflage	Nachweis offen	—	Update-Policy / Patch-Nachweis
Incident-Kontakt & Meldeweg	erfüllt laut Eingabe	Nachweis abgelegt	Netzlaufwerk/Compliance/Nachweise	Vertrag / Runbook
SLA / Supportweg	erfüllt laut Eingabe	Nachweis abgelegt	—	Vertrag / SLA-Dokument

KONTROLLPUNKT	BEWERTUNG	NACHWEIS	ABLAGEORT	NACHWEIS / QUELLE
Backup / Fallback	erfüllt laut Eingabe	Nachweis abgelegt	—	Notfall-/Fallback-Konzept
Supportzugriffe (EU/EWR) geregelt	erfüllt laut Eingabe	Nachweis abgelegt	—	Vertrag / Admin-Konfiguration
★ Training mit Kundendaten ausgeschlossen	erfüllt laut Eingabe	✓ Nachweis geprüft (laut Eingabe)	—	Vertrag / Anbieter-Bestätigung
Prompt-/Output-Speicherung geklärt	erfüllt mit Auflage	Nachweis offen	—	Anbieter-Konfiguration
Lösch-/Exportmöglichkeit	erfüllt laut Eingabe	Nachweis abgelegt	—	Lösch-/Exportkonzept
★ Mandantentrennung / Tenant Isolation	erfüllt laut Eingabe	✓ Nachweis geprüft (laut Eingabe)	—	Anbieter-Architektur-Doku

★ = kritischer Kontrollpunkt. Logik: kritischer Punkt **nicht erfüllt** ⇒ nicht freigabefähig · **offen** ⇒ Go-live-Auflage · **erfüllt laut Eingabe, Nachweis offen** ⇒ entscheidungsreif mit Go-live-Auflage · **erfüllt und Nachweis geprüft** ⇒ kein Hindernis.

A3c

Datensouveränität (Nachweis)

Belegt, **wo die Daten liegen** und dass die Auswertung selbst keine Daten abgibt. „Nein“/„unklar“-Punkte sind über die Auflagen (Abschnitt ②) vor dem Go-live zu schließen. Keine Rechtsberatung.

Methodik-Hinweis (Souveränität): Optionen mit Datenresidenz-Bedarf werden im Ranking **nicht automatisch ausgeschlossen**, sondern mit ⚠ markiert und als Auflage geführt — so bleibt die empfohlene Option sichtbar und Ihr Haus entscheidet nach Prüfung der Region/Vertragslage über einen endgültigen Ausschluss. Ein explizit verweigerter DE-/EU-Datenstandort (Eingabe „nein“) ist dagegen ein **harter Stopper**.

Geforderte Datenresidenz	EU/EWR
Verarbeitung durch dieses Werkzeug	regelbasiert & deterministisch — kein KI-Sprachmodell, keine Weitergabe an Dritte (Details A8). Ihre Eingaben werden zur Erzeugung dieses Berichts an den Server des Anbieters übertragen, dort verarbeitet und nicht gespeichert ; gespeichert wird ausschließlich auf Ihrem Rechner. Betrifft die Auswertung in diesem Werkzeug , nicht den späteren KI-Betrieb der gewählten Hosting-Option (dort kann je nach Option ein Datenabfluss entstehen — siehe Auflagen).
Empfohlene Option / Anbieter	Public Cloud · Microsoft Azure · EU (Frankfurt / Schweden)
Verarbeitungsregion vertraglich zugesichert (Belegenheitsort)	✓ ja
Übermittlungsgrundlage nach Kapitel V DSGVO (Art. 45 Angemessenheitsbeschluss / Art. 46 Standardvertragsklauseln / Art. 49)	zu belegen — siehe Freigabebedingung; eine EU-Region ersetzt die Übermittlungsgrundlage nicht
Transfer Impact Assessment durchgeführt (bei Standardvertragsklauseln)	zu belegen — siehe Freigabebedingung
Auftragsverarbeitungsvertrag (Art. 28 DSGVO)	ja, abgeschlossen

Subprozessoren offengelegt/geprüft	✓ ja
Support-Zugriff außerhalb EU/EWR	✓ keiner
Training mit eigenen/Kundendaten ausgeschlossen	✓ ja
Lösch-/Rückgabekonzept	✓ ja

A4

Detailprüfung Schritt 1 — Machbarkeit

Sieben Grundvoraussetzungen. Eine „nicht erfüllt“ hält die Entscheidung an, bis sie geklärt ist.

VORAUSSETZUNG	ANTWORT	STATUS
Technology — Datenverfügbarkeit	Ja, vollständig	✓ erfüllt
Organisation — Verantwortlicher	Ja, namentlich benannt	✓ erfüllt
Organisation — Prozesse	Ja, dokumentiert	✓ erfüllt
Environment — Regulatorik	Ja, vollständig	✓ erfüllt
Environment — Sektor	Ja, identifiziert und berücksichtigt	✓ erfüllt
Psychosocial — Vertrauen	Hoch, Unterstützung vorhanden	✓ erfüllt
Psychosocial — Change-Kapazität	Ja	✓ erfüllt

A5

Detailprüfung Schritt 2 — Verantwortung & Nachweis

Vier Routinen sichern den verantwortungsvollen Betrieb (Arbeitsvorlagen unter A6). Ein „Nein“ hält die Entscheidung an.
Wichtig zum Verständnis: Die Antworten hier sind Ihre **Selbstauskunft aus dem Formular** („ist der Prozess vorhanden?“). Ob eine Routine auch **durchgeführt und belegt** ist, zeigt allein das Routinen-Logbuch (A6a) mit datierten Einträgen und Reifegrad. Ein „Ja“ hier und „nicht eingerichtet“ dort ist deshalb kein Widerspruch, sondern der Unterschied zwischen Vorhaben und Nachweis.

Routine 1 — Risiko-Check vor dem Go-live (Fachreferenz: SOP 1, COBIT APO13)

CHECK	ANTWORT
Ist ein klarer Auslöser definiert — jedes Deployment bzw. Major Update löst die Risikobewertung aus?	✓ Ja
Werden vor Produktivnahme Bias-, Robustheits- und Adversarial-Tests durchgeführt?	✓ Ja
Werden Schwachstellen dokumentiert und Mitigationsmaßnahmen festgelegt (Risk-Register, Mitigationsplan)?	✓ Ja
Liegt prüffähige Evidenz vor (Risk-Report, Bias-Audit-Logs, unterschriebene Freigabe)?	✓ Ja

Verantwortliche/r: KI-Beauftragte, S. Musterfrau

Routine 2 — Fairness & Nachvollziehbarkeit im Betrieb (Fachreferenz: SOP 2, COBIT MEA03)

CHECK	ANTWORT
Werden Fairness- und Transparenzkennzahlen laufend überwacht (Drift, Bias, Erklärbarkeit via SHAP/LIME)?	✓ Ja
Ist eine feste Frequenz definiert (z. B. quartalsweise) plus Ad-hoc-Review nach Vorfällen?	✓ Ja

CHECK	ANTWORT
Werden Ergebnisse über Nutzergruppen verglichen und Anomalien dokumentiert/eskaliert?	✓ Ja
Liegt ein Evidence-Item vor (Compliance-Dashboard, Transparenz-Log, Fairness-Report-Archiv)?	✓ Ja

SOP 3 — Data & Model Change Control (BAI06/07)

CHECK	ANTWORT
Existiert ein Change-Control-Prozess (Versionierung, Validierung, Rollback) für Daten- und Modelländerungen?	✓ Ja
Wer gibt eine neue Modellversion produktiv frei (Change Advisory Board / benannte Rolle)?	✓ Ja
Werden Änderungen gestaffelt ausgerollt (Shadow/Canary) mit Drift- und Offline-Validierung?	✓ Ja
Liegen versionierte Artefakte plus CI/CD- und Test-Logs als Nachweis vor?	✓ Ja

Routine 4 — Störungen beheben & zurück auf sicheren Stand (Fachreferenz: SOP 4, COBIT DSS02)

CHECK	ANTWORT
Gibt es einen dokumentierten Incident-Pfad mit Severity-Klassifizierung (SEV-1 ... SEV-4)?	✓ Ja
Ist ein Rollback auf das letzte funktionierende Modell vorhanden und getestet?	✓ Ja
Ist die Eskalation bei Compliance-/Kundenimpact definiert (Geschäftsleitung, DSB, Aufsicht)?	✓ Ja
Erfolgt ein Post-Incident-Review mit CAPA-Maßnahmen (Corrective/Preventive Actions)?	✓ Ja

Offene Punkte

Keine offenen Punkte.

A5b

Konkrete Schritte je Freigabebedingung

Die Auflagen selbst stehen im Abschnitt „Freigabebedingungen“ (Entscheidungsteil). Hier folgen je Bedingung die Einzelschritte und die auszufüllenden Nachweis-Vorlagen — gedacht für Datenschutzbeauftragte, IT und Prüfer.

Pro Bedingung die Einzelschritte mit Abnahmekriterium und grobem Aufwand. **Haken Sie erledigte Schritte ab** — sie zählen in den Fortschritt (Dashboard) und werden gespeichert. **Sind alle Schritte einer Bedingung erledigt, gilt die Bedingung oben automatisch als erfüllt (●)**. Bedingungen, die auf eine laufende Betriebsroutine zurückgehen (z. B. Risiko-Check, Monitoring), verlinken auf die volle Arbeitsvorlage im Anhang; einmalige Aufgaben (Person benennen, AVV) haben keinen solchen Link. Vorschlag — im Workshop konkretisieren.

■ 1. Sign-off der/des Verantwortlichen einholen · Geschäftsführung · vor Go-live

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Decision Record der/dem benannten Verantwortlichen vorlegen.	Vorgelegt	gering
☐	Freigabe (Datum + Unterschrift) im Freigabe-Abschnitt erfassen.	Sign-off im Freigabe-Feld erfasst	gering

Dokumentiert die bewusste Freigabeentscheidung. Vor der Unterschrift prüfen:

- ☐ Alle Go-live-Auflagen erfüllt oder verbindlich terminiert
- ☐ Verantwortliche Person benannt
- ☐ Security-Baseline geprüft bzw. terminiert
- ☐ Budget/Ressourcen für den Betrieb geklärt

KI-Anwendung / Use-Case

Freigegebene Option

Geplanter Go-live (Datum)

Freigebende Person (Name)

Rolle / Funktion

Datum der Freigabe

„Ich gebe die o. g. KI-Anwendung unter den dokumentierten Auflagen zur Produktivnahme frei. Die offenen Go-live-Auflagen sind erfüllt bzw. verbindlich terminiert. Die nächste Entscheidungs-Review ist eingeplant.“

Vorbehalte / Auflagen mit Frist

Nächste Review (Datum)

Datum, Ort: _____ Unterschrift: _____

Muster/Orientierung —keine Rechtsberatung. Fertiges Dokument mit DSB/Anwalt finalisieren, nachvollziehbar ablegen und im Logbuch (©). Ablageort + Datum eintragen.

■ 2. Nachweis zur DE-/EU-Datenresidenz nachvollziehbar ablegen (EU) · IT-Leitung · vor Go-live

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Vertragsklausel/Bestätigung zur DE-/EU-Region nachvollziehbar ablegen.	Nachweis abgelegt	gering
☐	Subprozessoren-Liste auf Drittlandübermittlung prüfen und ablegen.	Subprozessoren geprüft & dokumentiert	mittel

Belegt, wo die Daten verarbeitet/gespeichert werden. „Nein“/„unklar“ vor Go-live klären.

Geforderte Region (z. B. DE, EU/EWR)

Anbieter / Dienst

Rechenzentrums-Standort(e)

- ☐ Region vertraglich/schriftlich zugesichert
- ☐ Subprozessoren-Liste geprüft – keine ungesicherte Drittlandverarbeitung
- ☐ Support-/Fernzugriffe auf EU/EWR begrenzt oder vertraglich abgesichert

Fundstelle Vertragsklausel / Bestätigung

Ablageort des Nachweises

Muster/Orientierung — **keine Rechtsberatung**. Fertiges Dokument mit DSB/Anwalt finalisieren, nachvollziehbar ablegen und im [Logbuch](#) (📖). Ablageort + Datum eintragen.

■ 3. Übermittlungsgrundlage für Drittländer festlegen und belegen (DSGVO Kapitel V) · DSB + Einkauf

· vor Go-live

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Feststellen, ob überhaupt eine Übermittlung in ein Drittland vorliegt — einschließlich Fernzugriff durch Support/Administration, Subprozessoren und Konzernmutter außerhalb des EWR.	Übermittlungsgrundlage schriftlich festgestellt	mittel
☐	Übermittlungsgrundlage bestimmen: Angemessenheitsbeschluss (Art. 45 — bei US-Empfängern die aktive Zertifizierung im EU-US Data Privacy Framework in der offiziellen Liste prüfen), Standardvertragsklauseln (Art. 46 Abs. 2 lit. c) oder ausnahmsweise Art. 49.	Grundlage benannt und belegt	mittel
☐	Bei Standardvertragsklauseln: Transfer Impact Assessment durchführen — Rechtslage im Empfängerland, Zugriffsmöglichkeiten von Behörden, Wirksamkeit der Garantien.	Transfer Impact Assessment dokumentiert	mittel
☐	Zusätzliche Maßnahmen festlegen, wo die Garantien allein nicht tragen (z. B. Verschlüsselung mit Schlüsselhoheit im Haus, Pseudonymisierung, Beschränkung des Supportzugriffs).	Zusätzliche Maßnahmen vereinbart und wirksam	mittel
☐	Übermittlungsgrundlage im Verzeichnis von Verarbeitungstätigkeiten (Art. 30 Abs. 1 lit. e) und in den Datenschutzhinweisen führen.	VVT und Hinweise aktualisiert	gering

■ 4. Unterzeichneten AVV nachvollziehbar ablegen · DSB / Einkauf · vor Go-live

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Unterzeichnete AVV-Fassung nachvollziehbar ablegen und im VVT referenzieren.	AVV abgelegt & referenziert	gering
☐	Prüfen, ob weitere externe Dienstleister personenbezogene Daten verarbeiten (z. B. E-Mail-/Kommunikations- oder Hosting-Anbieter) — auch dort einen AVV sicherstellen.	AVV auch für weitere Dienstleister vorhanden/geprüft	gering

Prüfraster für den Auftragsverarbeitungsvertrag nach Art. 28 DSGVO — **kein Vertragsersatz**. Der AVV selbst wird mit DSB/Anwalt finalisiert.

Anbieter / Auftragsverarbeiter

Vertragsdatum

Laufzeit / Kündigung

- ☐ Weisungsbindung (Anbieter handelt nur auf Ihre Weisung)
- ☐ Technisch-organisatorische Maßnahmen (TOM) angemessen
- ☐ Subprozessoren geregelt (Liste, Genehmigung, Info-Pflicht)
- ☐ Lösch-/Rückgabekonzept vorhanden
- ☐ Keine ungesicherte Drittlandübermittlung (Art. 44–49)
- ☐ Meldepflicht bei Datenschutzverletzungen geregelt
- ☐ Kontroll- / Auditrechte vereinbart
- ☐ Unterzeichnet & nachvollziehbar abgelegt

Ablageort / Referenz im VVT

Muster/Orientierung —**keine Rechtsberatung**. Fertiges Dokument mit DSB/Anwalt finalisieren, nachvollziehbar ablegen und im Logbuch (©). Ablageort + Datum eintragen.

■ 5. Personenbezug & besondere Kategorien dokumentieren · DSB · vor Go-live

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Verarbeitete Datenarten vollständig auflisten.	Liste vollständig	gering
☐	Personenbezug und besondere Kategorien (Art. 9) markieren.	Markierung erfolgt	gering
☐	Rechtsgrundlage je Verarbeitung bestimmen.	Rechtsgrundlage je Zweck dokumentiert	mittel
☐	Ins Verzeichnis von Verarbeitungstätigkeiten (VVT) eintragen.	VVT aktualisiert	gering

Eintrag für das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO).

Bezeichnung der Verarbeitung

Zweck der Verarbeitung

Datenkategorien

Betroffene Personen

Rechtsgrundlage (Art. 6, ggf. Art. 9)

Empfänger / Auftragsverarbeiter

Drittlandtransfer? (Garantien)

Löschfrist

Verweis auf TOM-Konzept

Verantwortlich / Ansprechpartner

Muster/Orientierung —keine Rechtsberatung. Fertiges Dokument mit DSB/Anwalt finalisieren, nachvollziehbar ablegen und im Logbuch (©), Ablageort + Datum eintragen.

■ 6. DSFA-Relevanz bewerten · DSB · vor Go-live

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Schwellwertprüfung nach Art. 35 durchführen.	Ergebnis (hohes Risiko ja/nein) dokumentiert	gering
☐	Bei hohem Risiko: DSFA erstellen und Schutzmaßnahmen ableiten.	DSFA-Dokument + Maßnahmen vorliegen	mittel
☐	DSB einbinden; Ergebnis und Begründung dokumentieren.	DSB-Stellungnahme abgelegt	gering

Schwellwertprüfung nach Art. 35 DSGVO. Trifft mind. ein Punkt zu (bzw. zwei Kriterien der Art.-29-Liste), ist eine Datenschutz-Folgenabschätzung i. d. R. erforderlich:

- ☐ Umfangreiche Verarbeitung besonderer Kategorien (Art. 9)
- ☐ Systematische, umfangreiche Überwachung / Profiling
- ☐ Neue Technologie mit voraussichtlich hohem Risiko
- ☐ Automatisierte Entscheidungen mit Rechtswirkung
- ☐ Daten schutzbedürftiger Personen (z. B. Beschäftigte)
- ☐ Zusammenführung / Abgleich von Datensätzen mehrerer Quellen

Betroffene Personengruppen

Ergebnis (DSFA erforderlich? ja / nein)

Begründung / nächste Schritte

Mit DSB abgestimmt am / durch

Muster/Orientierung —**keine Rechtsberatung**. Fertiges Dokument mit DSB/Anwalt finalisieren, nachvollziehbar ablegen und im [Logbuch](#) (©). Ablageort + Datum eintragen.

■ 7. Informationspflichten und Betroffenenrechte anpassen (DSGVO Art. 13/14) · DSB · vor Go-live

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Datenschutzhinweise für Kunden und Beschäftigte um die KI-gestützte Verarbeitung ergänzen: Zwecke, Rechtsgrundlage, Empfänger einschließlich Cloud-Anbieter, Drittlandbezug, Speicherdauer.	Hinweise aktualisiert und veröffentlicht	mittel
☐	Prüfen, ob Daten nicht bei der betroffenen Person erhoben werden (Art. 14) — dann zusätzlich Herkunft der Daten angeben und die Informationsfrist beachten.	Art.-14-Fall geprüft und dokumentiert	gering
☐	Prozess für Betroffenenanfragen (Auskunft Art. 15, Löschung Art. 17, Widerspruch Art. 21) auf die neue Verarbeitung erweitern — einschließlich der beim Anbieter liegenden Daten.	Auskunftsprozess deckt die KI-Verarbeitung ab	mittel
☐	Zuständigkeit und Antwortfrist (ein Monat, Art. 12 Abs. 3) intern festlegen.	Zuständigkeit und Frist benannt	gering

■ 8. Risiko-Check vor Produktivnahme abschließen · IT + Fachbereich · vor Go-live → volle Arbeitsvorlage:

[Routine 1 \(Anhang\)](#).

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Testfälle/Stichproben und Bias-Check durchführen.	Testlauf dokumentiert	mittel
☐	Ergebnisse bewerten; offene Risiken benennen.	Risikobewertung vorliegt	gering
☐	Freigabe durch Verantwortliche/n einholen.	Freigabe erteilt	gering
☐	Freigabeprotokoll ablegen.	Protokoll abgelegt	gering

Kurzbewertung der wichtigsten Betriebsrisiken vor dem Go-live.

Top-Risiken (Betrieb, Datenqualität, Fehlentscheidung, Verfügbarkeit/Ausfall)

Eintrittswahrscheinlichkeit (gering / mittel / hoch)

Auswirkung (gering / mittel / hoch)

Maßnahmen / Gegensteuerung

Ausfall- / Rollback-Plan (was, wenn es schiefgeht?)

- ☐ Menschliche Kontrolle der KI-Ergebnisse definiert
- ☐ Datenqualität geprüft

Restrisiko akzeptiert durch (Name)

Datum

Muster/Orientierung —keine Rechtsberatung. Fertiges Dokument mit DSB/Anwalt finalisieren, nachvollziehbar ablegen und im Logbuch (📁), Ablageort + Datum eintragen.

■ 9. Monitoring- & Incident-Prozess festlegen · IT-Leitung · Tag 30 → volle Arbeitsvorlage: Routine 4 (Anhang).

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Kennzahlen und Schwellen definieren (siehe KPI-Plan).	KPI + Schwellen definiert	gering
☐	Verantwortliche und Eskalationsweg benennen.	Eskalationsweg steht	gering
☐	Rückfall-/Notfallplan dokumentieren.	Notfallplan dokumentiert	mittel
☐	Erste Review terminieren.	Review-Termin steht	gering

Wie wird der Betrieb überwacht und auf Störungen/Vorfälle reagiert?

Was wird überwacht? (Qualität, Verfügbarkeit, Fehlerrate, Auffälligkeiten)

Prüf-Takt (z. B. wöchentlich)

Meldeweg bei Incident (an wen?)

Reaktions- / Meldefrist

Eskalations- & Behebungsschritte

☐ DSGVO-Meldepflicht (72 h, Art. 33) berücksichtigt

☐ Verantwortliche/r für Monitoring benannt

Ablageort Protokoll / Logbuch-Verweis

Muster/Orientierung —keine Rechtsberatung. Fertiges Dokument mit DSB/Anwalt finalisieren, nachvollziehbar ablegen und im Logbuch (©). **Ablageort + Datum eintragen.**

■ 10. NIS2-Betroffenheit feststellen und, falls zutreffend, Pflichten umsetzen · Geschäftsführung + IT-

Leitung · Tag 30

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Betroffenheit feststellen: Fällt die Tätigkeit unter die Sektorlisten des BSIG (Umsetzung der Anhänge I/II) und werden die Schwellenwerte erreicht (ab 50 Beschäftigte oder mehr als 10 Millionen Euro Jahresumsatz bzw. Bilanzsumme)? Ergebnis mit Begründung schriftlich festhalten — auch ein negatives Prüfergebnis ist ein Nachweis.	Betroffenheitsprüfung schriftlich dokumentiert	mittel
☐	Falls betroffen: Registrierung beim BSI vornehmen und die Registrierungsdaten aktuell halten.	Registrierung erfolgt, Bestätigung abgelegt	gering
☐	Meldeprozess mit den drei Fristen einrichten: Frühwarnung innerhalb von 24 Stunden, Meldung innerhalb von 72 Stunden, Abschlussbericht innerhalb eines Monats. Rufbereitschaft und Zuständigkeit benennen, damit die 24-Stunden-Frist auch außerhalb der Geschäftszeiten gehalten wird.	Meldeprozess dokumentiert, Zuständigkeit und Erreichbarkeit benannt	mittel
☐	Risikomanagement-Maßnahmen abgleichen (Art. 21 der Richtlinie, umgesetzt im BSIG): Risikoanalyse und Sicherheitskonzept, Bewältigung von Sicherheitsvorfällen, Backup und Krisenmanagement, Sicherheit der Lieferkette einschließlich Cloud-Anbieter, Sicherheit bei Beschaffung und Entwicklung, Wirksamkeitsprüfung, Cyberhygiene und Schulung, Kryptografie, Personalsicherheit und Zugriffskontrolle, Multi-Faktor-Authentifizierung und gesicherte Kommunikation.	Abgleich dokumentiert, Lücken mit Terminen hinterlegt	mittel
☐	Diese KI-Anwendung und den gewählten Hosting-Anbieter ausdrücklich in die Lieferketten-Betrachtung aufnehmen — NIS2 erfasst auch Dienstleister, die für den Betrieb wesentlich sind.	Anbieter in der Lieferketten-Übersicht geführt	gering

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Verantwortung der Geschäftsleitung beachten: Billigung und Überwachung der Maßnahmen sind Leitungsaufgabe und persönlich haftungsbewehrt; Schulung der Leitungsebene dokumentieren.	Billigung protokolliert, Schulung nachgewiesen	gering

■ 11. Vertraulichkeit & Geheimnisschutz prüfen · IT + Fachbereich · vor Go-live

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Schützenswerte Inhalte einstufen (Kundendaten, Geschäftsgeheimnisse).	Einstufung dokumentiert	gering
☐	Zugriff/Verschlüsselung und Geheimhaltung (NDA) regeln.	Zugriffs- und NDA-Regelung steht	mittel
☐	Prüfen, ob Inhalte an Anbieter/Modell gelangen — ggf. anonymisieren.	Datenfluss geprüft, ggf. anonymisiert	mittel

Schutz von Kundendaten und Geschäftsgeheimnissen (DSGVO Art. 32 / GeschGehG).

- ☐ Geheimhaltungsvereinbarung (NDA) mit Anbieter/Beteiligten vorhanden
- ☐ Zugriff auf Need-to-know beschränkt (Rollen/Rechte)
- ☐ Vertrauliche Inhalte gekennzeichnet / klassifiziert
- ☐ Keine vertraulichen Daten ungeschützt in Prompts/Training
- ☐ Verschlüsselung in Übertragung & Speicherung

Weitere Maßnahmen / Anmerkungen

Geprüft durch / Datum

Muster/Orientierung —**keine Rechtsberatung**. Fertiges Dokument mit DSB/Anwalt finalisieren, nachvollziehbar ablegen und im Logbuch (©). Ablageort + Datum eintragen.

■ 12. Security-Baseline-Nachweise ablegen und prüfen · IT-Leitung / Security · vor Go-live

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Mehr-Faktor-Authentifizierung (MFA) für alle Zugänge aktiviert.	MFA aktiv	gering
☐	Rollen-/Rechtekonzept (Least Privilege) festgelegt.	Rechtekonzept dokumentiert	mittel
☐	API-Keys sicher gespeichert (Secret-Store) und Rotation geregelt.	Keys im Secret-Store + Rotationsplan	mittel
☐	Verschlüsselung in Transit (TLS) und im Ruhezustand bestätigt.	Verschlüsselung bestätigt	gering
☐	Logging/Protokollierung aktiviert und Aufbewahrung geregelt.	Logging aktiv	gering
☐	Prompt-/Output-Speicherung beim Anbieter geklärt und konfiguriert.	Speicherung geklärt	gering
☐	Training mit Ihren Daten ausgeschlossen (vertraglich/konfiguriert).	Training-Ausschluss bestätigt	gering

✓	SCHRITT	FERTIG, WENN ...	AUFWAND
☐	Supportzugriffe (wer, woher, EU/EWR) geregelt.	Supportzugriffe geregelt	gering
☐	Incident-Kontakt und Meldeweg beim Anbieter dokumentiert.	Incident-Meldeweg steht	gering
☐	SLA (Verfügbarkeit, Reaktionszeiten) geprüft.	SLA geprüft	gering
☐	Notfall-/Fallback-Lösung bei Anbieterausfall festgelegt.	Fallback dokumentiert	mittel
☐	Datenexport/Portabilität (Exit) sichergestellt.	Export möglich	gering
☐	Ergebnis als Security-Checkliste/Nachweis ablegen.	Nachweis abgelegt	gering

Ergänzt die 18-Punkte-Security-Baseline (Anhang A3b): Nachweise je kritischem Punkt sammeln und ablegen.

- ☐ Alle kritischen (★) Kontrollpunkte erfüllt
- ☐ Nachweise (Konfigs, Screenshots, Richtlinien) abgelegt
- ☐ Zugriffs- / Rechtekonzept dokumentiert
- ☐ Backup/Restore getestet
- ☐ Verschlüsselung in Übertragung & Speicherung

Offene Punkte / Termin

Geprüft durch (IT/Security) / Datum

Ablageort der Nachweise

Muster/Orientierung —**keine Rechtsberatung**. Fertiges Dokument mit DSB/Anwalt finalisieren, nachvollziehbar ablegen und im Logbuch (©). Ablageort + Datum eintragen.

A6

Betriebsroutinen (Arbeitsvorlagen)

Wozu dieser Abschnitt? Dies sind **empfohlene Betriebs-Routinen**, die den laufenden, sicheren Betrieb Ihrer KI absichern (Risiko-Check, Monitoring, Änderungs- und Incident-Management). Sie sind **nicht Teil der Entscheidung selbst** und blockieren die Empfehlung nicht — sie sind Ihre Governance-Vorlage für die Zeit **nach** dem Go-live. Übernehmen Sie sie wie vorgeschlagen oder passen Sie sie an Ihre Organisation an.

Die vier Routinen sind aus den COBIT-2019-Kontrollzielen abgeleitet: Routine 1 = APO13 (Risk Control vor Deployment), Routine 2 = MEA03 (Monitoring & Fairness), Routine 3 = BAI06/07 (Change- & Datenmanagement), Routine 4 = DSS02 (Incident & Recovery). Hier sehen Sie je Routine, **was sie ist, wann sie nötig ist und wer sie verantwortlich** — die ausführliche Arbeitsvorlage für die IT ist je Routine ausklappbar. **Status, datierte Durchführungen und das Häkchen „als eingerichtet“ finden Sie im Abschnitt „© Logbuch“.**

Hinweis für kleinere SMEs: Die RACI-Rollen bezeichnen Verantwortlichkeiten, keine Stellen. In Firmen unter ~50 Mitarbeitern werden Rollen typisch gebündelt — die Geschäftsführung ist oft Accountable und Service Owner, ein IT-Generalist deckt AI Project Lead, MLOps Lead und Incident Manager ab, Legal/DSB wird extern bei Bedarf eingebunden. Wichtig ist nur, dass jede Verantwortlichkeit einer benannten Person zugeordnet bleibt.

Bei „Public Cloud“ verschiebt sich der Fokus so: Da die KI beim Anbieter läuft, drehen sich Ihre Routinen mehr um Verträge, Anbieter-Zusagen (SLA) und Protokolle als um eigene Technik. Bei Störungen (Routine 4) ist die Kernfrage: Wer eskaliert wann zum Anbieter?

Routine 1 — Risiko-Check, bevor eine KI live geht

regulatorisch veranlasst

nicht eingerichtet

→ Durchführungen erfassen / Historie (🔒 Logbuch)

Wann nötig: Deployment oder größeres Update eines KI-Modells. · **Wer verantwortlich:** KI-Beauftragte, S. Musterfrau · **Aufwand:** Beim ersten Mal ~1 Tag, bei späteren Updates 1–2 Stunden. · → im Formular (Schritt 2) bearbeiten

Was das für Ihre Firma heißt: Bevor eine neue KI live geht, einmal prüfen: Behandelt sie alle Kundengruppen fair, hält sie auch bei untypischen Eingaben stand, wo sind die Schwachstellen — und wer gibt das frei? Ergebnis auf einem Blatt festhalten.

Beispiel aus dem Alltag: Bevor Ihr neuer Angebots-Assistent live geht, lässt eine benannte Person ein paar Dutzend Testfälle durchlaufen und prüft, ob er bei verschiedenen Kundengruppen sachlich gleich antwortet. Ergebnis auf ein Blatt, die Geschäftsführung gibt frei.

Was auf Ihrem Tisch landet: Vor dem Live-Gang bekommen Sie eine kurze Freigabe-Vorlage (Test bestanden ja/nein · gefundene Risiken · Empfehlung) und entscheiden: freigeben oder nicht.

⚠ **Wenn es nicht passt:** Fällt der Check durch, geht die KI nicht live — die verantwortliche Person stoppt den Go-live und informiert die Geschäftsführung.

Fachreferenz: SOP 1 — Algorithmische Risikobewertung (APO13-AI)

Praxis-Anpassung für zugekaufte KI-Dienste (SaaS/API):

- Bei zugekaufter KI statt eigener Trainingsdaten: Anbieter-Datenblatt/Model-Card, Auftragsverarbeitungsvertrag (AVV) und eigene Testfälle (Golden Set) als Grundlage nehmen.
- Datenabfluss prüfen: Welche (Kunden-)Daten gehen an welchen Anbieter? Werden sie zum Training genutzt? Zero-Retention bzw. EU-Region vertraglich klären.
- Robustheit heißt bei zugekaufter KI vor allem: Prompt-Injection bzw. manipulative Eingaben testen und Halluzinationen/Faktentreue stichprobenartig prüfen.
- API-Zugangsschlüssel sicher verwahren (kein Klartext, Rotation, Missbrauch bei Leck bedenken).

WOFÜR	Algorithmus-spezifische Risiken identifizieren und mindern (Bias, Robustheit, Adversarial-Exposition).
WANN STARTEN	Deployment oder größeres Update eines KI-Modells.
WAS SIE BRAUCHEN	Modelldokumentation, Trainings-/Testdaten, Risk-Register.
WAS DABEI RAUSKOMMT	Aktualisiertes Risk-Register, Mitigationsplan, Audit-Log.
WIE OFT	Verpflichtend bei jedem Modell-Release; jährliche Review.
NACHWEIS AUS	Risikobewertungs-Bericht, Bias-Audit-Logs, unterschriebene Freigabe.
BENANNTE/R VERANTWORTLICHE/R	KI-Beauftragte, S. Musterfrau

Wer macht was

MACHT'S	VERANTWORTET	WIRD GEFRAGT	WIRD INFORMIERT
AI Project Lead	CIO/CTO	Legal/Compliance	End-Nutzer

Ablauf-Checkliste

- ☐ Bias-Audit durchführen
- ☐ Robustheitstests
- ☐ Schwachstellen dokumentieren
- ☐ Mitigationsmaßnahmen festlegen

Nachweise dokumentieren Sie pro Durchführung im Routinen-Logbuch (Abschnitt A6a). Die routinenspezifischen Nachweisfelder dieser Routine sind dort in jedem datierten Eintrag enthalten.

Routine 2 — Fairness & Nachvollziehbarkeit im Betrieb empfohlene Praxis

nicht eingerichtet → [Durchführungen erfassen / Historie \(📄 Logbuch\)](#)

Wann nötig: Sobald das KI-System produktiv ist. · **Wer verantwortet:** CEO/Geschäftsleitung · **Aufwand:** Etwa 2–3 Stunden pro Quartal. · → im Formular (Schritt 2) bearbeiten

Was das für Ihre Firma heißt: Vierteljährlich stichprobenartig nachsehen: Entscheidet die KI bei verschiedenen Kundengruppen vergleichbar, und kann man nachvollziehen, warum sie etwas vorschlägt? Auffälligkeiten notieren und melden.

Beispiel aus dem Alltag: Einmal im Quartal zieht jemand 10 echte KI-Antworten und prüft: Sind die fair? Lässt sich erklären, warum die KI das vorgeschlagen hat? Auffälligkeiten kommen ins Protokoll.

Was auf Ihrem Tisch landet: Sie erhalten im vereinbarten Takt einen kurzen Statusbericht (läuft fair und stabil ja/nein · Auffälligkeiten).

⚠ **Wenn es nicht passt:** Bei Auffälligkeiten wird nachgesteuert; wiegt es schwer, informiert die verantwortliche Person die Geschäftsführung und schlägt Maßnahmen vor.

Fachreferenz: SOP 2 — Fairness- & Transparenz-Monitoring (MEA03-AI)

Praxis-Anpassung für zugekaufte KI-Dienste (SaaS/API):

- SHAP/LIME nur bei selbst betriebenem Modell. Bei zugekaufter KI: begründete Stichprobe der Ausgaben auf Fairness und Faktentreue durchsehen, Auffälligkeiten dokumentieren.
- Menschliche Kontrolle (EU AI Act Art. 14): festlegen, wer eingreifen oder übersteuern darf — und solche Eingriffe protokollieren.
- Transparenz hat zwei Seiten: intern (warum schlägt die KI etwas vor?) und gegenüber Nutzern (Kennzeichnung, dass KI im Spiel ist — EU AI Act Art. 50). Art. 13 richtet sich dagegen an Anbieter von Hochrisiko-Systemen und begründet für Sie als Betreiber keine eigene Kennzeichnungspflicht.
- Verantwortung: laufendes Monitoring liegt bei Fachbereich/IT; der/die Datenschutzbeauftragte berät (nicht ausführend).

WOFÜR	Fairness und Transparenz der KI-Ausgaben überwachen, um Compliance und Stakeholder-Vertrauen zu sichern.
WANN STARTEN	Sobald das KI-System produktiv ist.
WAS SIE BRAUCHEN	Output-Logs, Explainability-Berichte, Feedback-Formulare.
WAS DABEI RAUSKOMMT	Transparenz-Log, quartalsweiser Fairness-Bericht, Korrekturmaßnahmen.
WIE OFT	Quartalsweise, mit Ad-hoc-Review nach größeren Vorfällen.
NACHWEIS AUS	Compliance-Dashboard, audit-fähige Logfiles, Fairness-Bericht-Archiv.

Wer macht was

MACHT'S	VERANTWORTET	WIRD GEFRAGT	WIRD INFORMIERT
Datenschutzbeauftragte/r	CEO/Geschäftsleitung	Fachexperten	Nutzer

Ablauf-Checkliste

- ☐ Quartalsweise Fairness-Review
- ☐ SHAP/LIME-Erklärungen erzeugen
- ☐ Ergebnisse über Nutzergruppen vergleichen
- ☐ Anomalien dokumentieren und eskalieren

Nachweise dokumentieren Sie pro Durchführung im Routinen-Logbuch (Abschnitt A6a). Die routinenspezifischen Nachweisfelder dieser Routine sind dort in jedem datierten Eintrag enthalten.

Routine 3 — Änderungen an Daten & Modell kontrollieren empfohlene Praxis

nicht eingerichtet → [Durchführungen erfassen / Historie \(📄 Logbuch\)](#)

Wann nötig: Geplante Änderung an Trainingsdaten, Feature-Store, Preprocessing, Modellparametern/-architektur oder Serving-Konfiguration. · **Wer verantwortlich:** Product Owner · **Aufwand:** Pro Änderung ~1–2 Stunden; kleine Änderungen weniger. · → im Formular (Schritt 2) bearbeiten

Was das für Ihre Firma heißt: Niemand ändert Daten oder das Modell 'mal eben'. Jede Änderung wird kurz dokumentiert, getestet und freigegeben — immer mit einem Rückweg, falls es schiefgeht.

Beispiel aus dem Alltag: Will jemand das Modell oder die zugrunde liegenden Daten ändern, schreibt er kurz auf was und warum, testet es abseits vom Echtbetrieb, jemand gibt frei — und es bleibt ein Weg zurück auf den alten Stand.

Was auf Ihrem Tisch landet: Größere Änderungen an Daten oder Modell werden der benannten Stelle zur Freigabe vorgelegt, bevor sie produktiv gehen.

⚠ Wenn es nicht passt: Ist eine Änderung riskant oder unklar, wird sie zurückgestellt — nichts geht ungeprüft live.

Fachreferenz: SOP 3 — Daten- & Modell-Change-Control (BAI06/BAI07-AI)

Praxis-Anpassung für zugekaufte KI-Dienste (SaaS/API):

- Bei zugekaufter KI ändern Sie nicht das Modell selbst, sondern Prompts/System-Prompts, hinterlegte Dokumente (RAG) und die gewählte Modell-Version des Anbieters — genau diese Änderungen kontrollieren.
- Statt Holdout/Cross-Validation: feste Test-Prompts mit Erwartungswerten (Golden Tests) vor und nach der Änderung laufen lassen.
- Statt eigenem Change-Advisory-Board: im KMU genügt eine Vier-Augen-Freigabe durch eine zweite benannte Person.
- Wichtig: Der Anbieter aktualisiert sein Modell evtl. still. Modell-Version festnageln (Pinning) wo möglich, und nach Anbieter-Updates die Golden Tests erneut laufen lassen.
- Große Änderung (major) = Verhalten, Qualität oder Rechtslage betroffen → dann den Risiko-Check (Routine 1) erneut auslösen; kleine (minor) = kosmetisch.

WOFÜR	Kontrollierte, auditierbare Änderungen an Datenpipelines, Features und Modellen; verhindert Regressionen und unbeabsichtigten Bias-Drift.
WANN STARTEN	Geplante Änderung an Trainingsdaten, Feature-Store, Preprocessing, Modellparametern/-architektur oder Serving-Konfiguration.
WAS SIE BRAUCHEN	Change-Request (CR), Model-Card, Data-Lineage, Validierungsplan, Risikobewertung.
WAS DABEI RAUSKOMMT	Freigegebener CR mit Sign-offs, Validierungsbericht, aktualisierte Model-Card, Release-Notes, Roll-back-Plan.
WIE OFT	Bei jeder Änderung; CAB wöchentlich oder ad hoc bei dringenden Änderungen.
NACHWEIS AUS	Versionierte Artefakte (Code, Data-Snapshots, Modell-Binaries), CI/CD-Logs, Test-Berichte, Freigaben im CR-System.

Wer macht was

MACHT'S	VERANTWORTET	WIRD GEFRAGT	WIRD INFORMIERT
MLOps Lead	Product Owner	Data Owner, Security Officer	Stakeholder

Ablauf-Checkliste

- ☐ CR triagieren und Impact klassifizieren (minor/major)
- ☐ Daten- & Label-Drift-Checks
- ☐ Offline-Validierung (Holdout, Cross-Val)
- ☐ Fairness-/Robustheitstests
- ☐ Security-Review
- ☐ Change-Advisory-Board-Freigabe für Major Changes
- ☐ Gestaffelter Rollout (Shadow/Canary)
- ☐ Post-Deployment-Monitoring

Nachweise dokumentieren Sie pro Durchführung im Routinen-Logbuch (Abschnitt A6a). Die routinenspezifischen Nachweisfelder dieser Routine sind dort in jedem datierten Eintrag enthalten.

Routine 4 — Störungen beheben & auf sicheren Stand zurück regulatorisch veranlasst

nicht eingerichtet → [Durchführungen erfassen / Historie \(📄 Logbuch\)](#)

Wann nötig: SLO/SLA-Verletzung, Anomalie-Alerts (Qualität/Fairness/Robustheit), Verdacht auf Datenleck, Modell-Degradation oder Nutzerbeschwerden. · **Wer verantwortlich:** Service Owner · **Aufwand:** Vorbereitung (Plan + Kontakte) ~½ Tag; im Ernstfall sofort. · → im Formular (Schritt 2) bearbeiten

Was das für Ihre Firma heißt: Wenn die KI Mist baut oder ausfällt: Wer wird wann alarmiert, wie schalten wir schnell auf den letzten funktionierenden Stand zurück — und was lernen wir daraus, damit es nicht wieder passiert?

Beispiel aus dem Alltag: Liefert die KI plötzlich Unsinn oder fällt aus: Die festgelegte Person wird alarmiert, schaltet auf den letzten funktionierenden Stand zurück, danach kurz festhalten: Was war die Ursache, was ändern wir?

Was auf Ihrem Tisch landet: Im Störfall bekommen Sie eine kurze Meldung (was ist passiert · Auswirkung · Sofortmaßnahme).

⚠ Wenn es nicht passt: Bei einem ernsten Vorfall wird auf den letzten funktionierenden Stand zurückgerollt und die Geschäftsführung umgehend informiert.

Fachreferenz: SOP 4 — Incident-Management & Modell-Rollback (DSS02-AI)

Praxis-Anpassung für zugekaufte KI-Dienste (SaaS/API):

- Rollback bei reiner API ist oft nicht zurück aufs alte Modell möglich. Realistisch: auf eine ältere, noch angebotene Modell-Version umschalten, die KI per Schalter (Feature-Flag) abschalten, oder auf manuellen/lokalen Notbetrieb ausweichen.
- Bei Ausfall der Anbieter-API: Eskalationsweg zum Anbieter (Support/SLA/Statusseite) festhalten — eigenes Drosseln hilft dann nicht.
- Schweregrade kurz definieren: SEV-1 = kritisch/Totalausfall, SEV-2 = stark eingeschränkt, SEV-3 = spürbar, SEV-4 = gering.
- Meldepflicht prüfen: bei Datenleck DSGVO Art. 33 (Meldung an die Aufsicht binnen 72 Stunden) und Art. 34 (Benachrichtigung der Betroffenen bei hohem Risiko); bei Hochrisiko-KI zusätzlich die Meldekette nach EU AI Act Art. 26 Abs. 5 (Betreiber informiert Anbieter und Behörde; Art. 73 selbst verpflichtet den Anbieter). Ergebnis festhalten (Meldung nötig? erfolgt?).

WOFÜR	KI-bezogene Vorfälle (Qualität, Fairness, Security, Verfügbarkeit) erkennen, eindämmen, lösen und sicheren Betrieb per kontrolliertem Rollback wiederherstellen.
WANN STARTEN	SLO/SLA-Verletzung, Anomalie-Alerts (Qualität/Fairness/Robustheit), Verdacht auf Datenleck, Modell-Degradation oder Nutzerbeschwerden.
WAS SIE BRAUCHEN	Monitoring-Alerts, Incident-Ticket, jüngste Deployments, Logs (Predictions, Explanations), Audit-Trail.
WAS DABEI RAUSKOMMT	Incident-Bericht (Timeline, Impact, RCA), Rollback-Bestätigung, CAPA-Backlog, Stakeholder-Kommunikation.
WIE OFT	Bei jedem Vorfall; Post-Incident-Review innerhalb von 5 Arbeitstagen nach Abschluss.
NACHWEIS AUS	Ticketing-System-Records, Alert-Dashboards, Rollback-Logs, Sign-offs, archivierte Stakeholder-Kommunikation.

Wer macht was

MACHT'S	VERANTWORTET	WIRD GEFRAGT	WIRD INFORMIERT
Incident Manager	Service Owner	MLOps Lead, DSB/Security, Legal	betroffene Nutzer

Ablauf-Checkliste

- ☐ Schweregrad klassifizieren (SEV-1 ... SEV-4)
- ☐ On-Call-Team einbinden
- ☐ Eindämmen (Traffic drosseln, Feature-Flag)
- ☐ Root-Cause-Analyse (Daten, Modell, Infra)
- ☐ Bei Bedarf Rollback auf letztes funktionierendes Modell
- ☐ Wiederherstellung validieren
- ☐ CAPA (Corrective/Preventive Actions) entwerfen
- ☐ Post-Incident-Review

Nachweise dokumentieren Sie pro Durchführung im Routinen-Logbuch (Abschnitt A6a). Die routinenspezifischen Nachweisfelder dieser Routine sind dort in jedem datierten Eintrag enthalten.

Governance-Fälligkeiten & Erinnerungen

0 überfällig/heute · 0 in den nächsten 30 Tagen · 0 aktuell

ROUTINE	VERANTWORTLICH	LETZTE	NÄCHSTE FÄLLIG	STATUS
1 Risiko-Check	—	—	—	keine Fälligkeit
2 Fairness & Nachvollziehbarkeit	—	—	—	keine Fälligkeit
3 Change Control	—	—	—	keine Fälligkeit
4 Incident & Rollback	—	—	—	keine Fälligkeit

Alles lokal in Ihrem Browser — keine Cloud, keine Datenübertragung.

A6a · Routinen-Logbuch (datierte Durchführungen) [↗ als eigene Seite öffnen](#)

Im Abschnitt „🕒 Routinen“ sehen Sie je Routine nur den **aktuellen Status** — hier stehen die **Status-Übersicht** (Tabelle unten) und die **vollständige, datierte Historie** jeder Durchführung.

Betriebsroutinen sind **wiederkehrende** Nachweise. Dokumentieren Sie hier jede Durchführung mit Datum, Anlass, Ergebnis und Nachweis. Die Einträge werden **lokal in Ihrem Browser** gespeichert und beim „Stand speichern“ in die Audit-Datei übernommen. **Status-Logik:** 🟢 aktuell · 🟡 fällig bald (≤14 T) / offene Punkte / Nachweis fehlt / bei regulatorischen Routinen (Risiko-Check, Incident): Nachweis empfohlen · 🔴 überfällig / nicht bestanden / kritisch · ⚪ nicht eingerichtet · □ nicht anwendbar (mit Begründung).

Reifegrad (0–3): 0 = nicht vorhanden · 1 = definiert, aber Lauf nicht bestanden/kritisch · 2 = eingerichtet & durchgeführt (Nachweis fehlt noch) · 3 = nachgewiesen (bestanden + Nachweis abgelegt). Ausführlich im Glossar (Anhang) und im [User Guide](#).

ROUTINE	REIFE	STATUS	LETZTE	NÄCHSTE	OFFEN	VERANTWORTLICH
1 · Risiko-Check	0	nicht eingerichtet	—	—	—	—
2 · Fairness & Nachvollziehbarkeit	0	nicht eingerichtet	—	—	—	—
3 · Change Control	0	nicht eingerichtet	—	—	—	—
4 · Incident & Rollback	0	nicht eingerichtet	—	—	—	—

Routine 1 · Risiko-Check vor Produktivnahme ⚪ nicht eingerichtet

[↑ Status setzen & Beschreibung \(Abschnitt 🕒\).](#)

Noch keine Durchführung dokumentiert. Vor Produktivnahme bzw. gemäß Review-Takt nachzuholen.

Routine 2 · Fairness & Nachvollziehbarkeit ⚪ nicht eingerichtet

[↑ Status setzen & Beschreibung \(Abschnitt 🕒\).](#)

Noch keine Durchführung dokumentiert. Vor Produktivnahme bzw. gemäß Review-Takt nachzuholen.

Routine 3 · Änderungen an Daten & Modell (Change Control) ⚪ nicht eingerichtet

[↑ Status setzen & Beschreibung \(Abschnitt 🕒\).](#)

Noch keine Durchführung dokumentiert. Vor Produktivnahme bzw. gemäß Review-Takt nachzuholen.

Routine 4 · Incident & Rollback

[↑ Status setzen & Beschreibung \(Abschnitt 4\).](#)

Noch keine Durchführung dokumentiert. Vor Produktivnahme bzw. gemäß Review-Takt nachzuholen.

A7

Laufende Überwachung (Kennzahlen)

★ = die 5 für den Anfang (ohne Spezial-Software messbar). Zielwerte sind Start-Empfehlungen; die Ampel setzt sich beim Eintragen automatisch. „Bei Rot“ sagt direkt, was zu tun ist.

KENNZAHL (★ = START)	ZIELWERT (START)	IST	STATUS	WER MISST	QUELLE · TAKT	BEI ROT TUN
★ Läuft die KI zuverlässig? (Verfügbarkeit/Monat ggü. Provider-SLA) Technology & Architecture	≥ 99 % · gelb 97–99 % · rot < 97 %	%	—	IT-Verantwortliche/r	Monitoring / Provider-Statusseite · monatlich	Vorfall aufnehmen, auf letzten funktionierenden Stand zurück (Routine 4)
★ Sind die Pflicht-Nachweise aktuell da? (Audit-Bereitschaft) Risk & Compliance / Security	100 % vorhanden · rot: kritische fehlen	% vorhanden	—	Geschäftsführung + externe/r DSB	Nachweis-Checkliste aus Schritt 2 · quartalsweise	fehlende Nachweise nachziehen (Routine 1 Risiko-Check / Routine 2 Fairness)
★ Geht etwas schief? (ernste KI-Vorfälle / Quartal) Risk (Restrisiko)	0 · gelb 1 · rot ≥ 2 oder 1 mit Kunden-impact	Anzahl/Quartal	—	IT + Geschäftsführung	Incident-/Ticketliste · monatlich	Vorfall aufnehmen, Ursache klären, ggf. zurückrollen (Routine 4)
★ Bleibt es im Budget? (Budgettreue — qualitativ) Economic (Financial)	Kosten bleiben im geplanten Rahmen; bei Überschreitung Ursache prüfen und gegensteuern (qualitative Einschätzung, keine Zielzahl)		—	Controlling / kaufm. Leitung	Buchhaltung + Budgetplan · quartalsweise	Kosten prüfen, ggf. Option/Architektur neu bewerten

KENNZAHL (★ = START)	ZIELWERT (START)	IST	STATUS	WER MISST	QUELLE · TAKT	BEI ROT TUN
★ Ist jemand zuständig? (jede KI hat benannten Owner) Organisation	100 % · rot: KI ohne Owner im Einsatz	% mit Owner	—	Geschäftsführung	Governance-Liste aus Schritt 1/2 · quartalsweise	eine/n Verantwortliche/n benennen
Bringt's dem Kunden was? (Zufriedenheit / Bearbeitungszeit) Market / Customer	messbare Verbesserung ggü. Start · rot: Beschwerden steigen	Score / %	—	Vertrieb / Kundenservice	CRM / Kundenfeedback · quartalsweise	Use-Case mit Vertrieb/Service prüfen
Sind die Leute befähigt? (Anteil geschulter Mitarbeiter) Personnel / Learning	≥ 80 % · gelb 50–80 % · rot < 50 %	% geschult	—	Personalleitung / Teamleiter	Schulungsliste · quartalsweise	Schulung nachziehen
Wie schnell von Idee zu Nutzen? (Time-to-Value) Innovation	Trend sinkend · rot: Projekte bleiben monatelang stecken	Tage	—	IT / Projektleitung	Projekt-/Delivery-Übersicht · quartalsweise	Engpass im Änderungsprozess beheben (Routine 3)

KPI-Historie (datierte Messrunden — Trend über die Zeit)

Tragen Sie oben die aktuellen Ist-Werte ein und sichern Sie sie als **Messrunde mit Stichtag** (z. B. quartalsweise, gemäß Review-Takt). So entsteht eine datierte Historie mit Ampel-Trend; sie wird im Browser gespeichert und in die Audit-Datei übernommen.

Noch keine Messrunde erfasst. Tragen Sie oben die Ist-Werte ein und klicken Sie „Kennzahlen erfassen“.

A8

Wie dieses Werkzeug arbeitet

Die Auswertung erfolgt **vollständig regelbasiert und nachvollziehbar**: Die Entscheidungs-Engine rechnet mit fester Mathematik (gewichtete Summen je Option, Schwellenwerte für die Schritte 1 und 2) — gleiche Eingaben ergeben immer das selbe Ergebnis. Der Interpretations-Abschnitt („Was bedeutet das für Sie?“) wird ebenfalls **regelbasiert aus den berechneten Werten** erzeugt. Es kommt **kein KI-Sprachmodell** zum Einsatz und es werden **keine Daten an Dritte übermittelt**. Ihre Eingaben werden zur Erzeugung dieses Berichts an den **Server des Anbieters** übertragen, dort verarbeitet und **nicht gespeichert** — dieselbe Verarbeitung, die Abschnitt A3c ausweist; gespeichert wird ausschließlich auf Ihrem Rechner. Damit bleibt jede Aussage des Berichts prüfbar und auf die Eingaben rückführbar.

A9

Nachvollziehbarkeit (Audit-Trail)

- Schritt 1 + 2 bestanden; Schritt 3 als gewichtete AHP-Bewertung ausgewertet.
- Souveränitäts-Filter aktiv (Datenresidenz: EU).

- Schritt 3 — höchste gewichtete Gesamtbewertung: **Public Cloud** (4,44); nächstbewertete Option: **Private Cloud** (3,79); Abstand 0,64 → Belastbarkeit „stark“
- Am höchsten gewichtete Kriterien: Technische Passung (30,6 %), Organisatorische Passung (21,4 %), Wirtschaftlichkeit (16,8 %) (Standard n=93)

Vertragsgrundlage: Vertragspartei ist **Beispiel GmbH**, handelnd durch **IT-Leitung, M. Mustermann**. Für dieses Unternehmen wurden die Nutzungsbedingungen und der Vertrag über die Auftragsverarbeitung (Fassung 1.1 (Stand 09/2026)) am **7.8.2026, 11:00:00** bestätigt; dabei wurde erklärt, dass das Unternehmen als Unternehmer im Sinne des § 14 BGB handelt (lizenzierter Zugang: Test endet in 3 Tagen). Dieser Eintrag ist der Nachweis des Vertragsschlusses; beide Dokumente sind unter tojonavigator.de/agb.html und [/avv.html](http://avv.html) abrufbar.

Erstellt mit **ToJo 1.22.3** · Datenschema **v7** · erzeugt am 22.09.2026. **Schritt-3-Eingabe-Modus:** Standard — Ausgangspunkt waren die modellhaften Startwerte des Bewertungsmodells (keine erhobenen Kennzahlen); welche Rohwerte davon abweichen, weist die Bewertungsmatrix zellengenau aus (S = Startwert, E = angepasst). Beim Laden einer gespeicherten Datei werden Herkunft (Speicherdatum, Version) und etwaige automatische Migrationen im Formular-Lade-Banner ausgewiesen.

A10

Glossar

BEGRIFF	BEDEUTUNG
Hauptzugang (Besitzer der Datei)	Der erste Zugang, der die Verschlüsselung einrichtet — der Besitzer der Datei. Nur er darf Zugänge verwalten (Mitglieder anlegen/entfernen, PINs zurücksetzen).
Notfall-Code (Recovery)	Einmalig angezeigter Wiederherstellungs-Code. Öffnet die Datei, wenn ein PIN vergessen wurde, und gilt als Notfall-Hauptschlüssel. Sicher aufbewahren — ohne ihn UND ohne PIN sind die Daten unwiederbringlich.
PIN	Persönliche Geheimzahl bzw. Kennwort (mind. 6 Zeichen, nicht nur Ziffern) zum Öffnen der verschlüsselten Datei.
Unterschrift (Signatur)	Digitale Unterschrift — belegt kryptografisch, welcher Zugang einen gespeicherten Stand erzeugt hat.
Decision Record	Strukturierte Entscheidungs- und Dokumentationsvorlage zur KI-Hosting-Frage.
Use Case	Der konkrete KI-Anwendungsfall — was die KI für wen tut.
On-Prem	Betrieb auf eigenen Servern im eigenen Haus (statt beim Cloud-Anbieter).
Reifegrad	Entwicklungsstand einer Betriebsroutine: 0 = nicht vorhanden, 1 = definiert, 2 = eingerichtet, 3 = nachgewiesen.
Belastbarkeit / Abstand	Wie klar Platz 1 vor Platz 2 liegt (Abstand der gewichteten Punktwerte): > 0,5 stark, 0,2–0,5 solide, 0,05–0,2 knapp, < 0,05 keine eindeutige Empfehlung.
Freigabebedingung (Go-live-Auflage)	Auflage, die vor der Produktivnahme zu erfüllen und zu belegen ist.
Stopper	Kritischer Punkt, der eine Freigabe hart blockiert (z. B. kein AVV bei personenbezogenen Daten).
Go-live	Der Tag, an dem die KI produktiv eingesetzt wird — im Bericht auch Produktivnahme genannt.
Sign-off	Förmliche Freigabe-Unterschrift der verantwortlichen Person.
Audit-Trail	Lückenlose, nachvollziehbare Begründungskette, wie die Empfehlung zustande kam.
Evidence-/Control-Matrix	Zuordnung von Auflagen/Aussagen zu ihren Nachweisen, Verantwortlichen und Fristen.
DSGVO	Datenschutz-Grundverordnung der EU — regelt den Umgang mit personenbezogenen Daten.

BEGRIFF	BEDEUTUNG
DSB (Datenschutzbeauftragte/r)	Interne oder externe Person, die die Einhaltung des Datenschutzes überwacht.
AVV (Auftragsverarbeitungsvertrag)	Vertrag nach Art. 28 DSGVO, der regelt, wie ein Dienstleister personenbezogene Daten in Ihrem Auftrag verarbeitet.
DSFA (Datenschutz-Folgenabschätzung)	Prüfung nach Art. 35 DSGVO, ob eine Verarbeitung ein hohes Risiko für Betroffene birgt und welche Maßnahmen das senken.
VVT (Verzeichnis von Verarbeitungstätigkeiten)	Pflicht-Verzeichnis der Datenverarbeitungen nach Art. 30 DSGVO.
Datenresidenz	Der geografische Ort, an dem Daten gespeichert und verarbeitet werden (z. B. Deutschland, EU).
EU AI Act	EU-Verordnung zur Regulierung von KI; teilt Anwendungen in Risikoklassen (verboten, hoch, begrenzt, minimal) mit unterschiedlichen Pflichten ein.
Anbieter / Betreiber	Anbieter entwickelt/bringt eine KI in Verkehr; Betreiber setzt sie in eigener Verantwortung ein.
High-Risk	Hochrisiko-KI im Sinne des AI Act (z. B. Personalauswahl, Kredit scoring) — strengere Pflichten.
Public Cloud	Betrieb beim Anbieter auf geteilter Infrastruktur.
Private Cloud	Dedizierte Cloud-Umgebung für ein Unternehmen.
Hybrid	Kombination aus Cloud und On-Prem (Schnitt legen Sie fest).
AlaaS (AI as a Service)	Nutzung eines fertigen KI-Dienstes über eine Schnittstelle (API), ohne eigenes Modell zu betreiben.
Betriebsroutine	Wiederkehrender Governance-Nachweis im laufenden Betrieb (die vier Routinen).
SOP (Standard Operating Procedure)	Standardisierte Arbeitsanweisung — hier die vier Betriebsroutinen.
RACI	Rollenmodell: Responsible (macht es), Accountable (verantwortet), Consulted (wird gefragt), Informed (wird informiert).
KPI (Key Performance Indicator)	Kennzahl zur laufenden Betriebsüberwachung (grün/gelb/rot).
SHAP / LIME	Zwei Verfahren, die sichtbar machen, welche Eingaben eine KI-Ausgabe wie stark beeinflusst haben (Erklärbarkeit). Nur bei selbst betriebenen Modellen anwendbar; bei zugekauften Diensten tritt eine Stichprobenprüfung an ihre Stelle.
Prompt-Injection	Manipulierte Eingabe, die die KI dazu bringt, ihre Anweisungen zu ignorieren — z. B. versteckter Text in einem hochgeladenen Dokument.
Halluzination	Eine erfundene, aber überzeugend formulierte KI-Ausgabe: sachlich falsch, sprachlich einwandfrei.
Modell-Drift	Nachlassende Ausgabequalität über die Zeit, weil sich Daten, Nutzung oder das Anbieter-Modell verändert haben.
Zero-Retention	Vertragliche Zusage des Anbieters, Ihre Eingaben nicht zu speichern und nicht zum Training zu verwenden.
Vendor-Lock-in	Abhängigkeit von einem Anbieter, die einen späteren Wechsel aufwendig oder teuer macht.
Angemessenheitsbeschluss (Art. 45 DSGVO)	Feststellung der EU-Kommission, dass ein Drittland ein angemessenes Datenschutzniveau bietet; dann ist eine Übermittlung ohne weitere Garantien zulässig.
Standardvertragsklauseln (SCC)	Von der EU-Kommission vorgegebene Vertragsklauseln, die eine Datenübermittlung in ein Drittland absichern (Art. 46 DSGVO).

BEGRIFF	BEDEUTUNG
Transfer Impact Assessment	Prüfung, ob die Standardvertragsklauseln im Empfängerland tatsächlich tragen — Rechtslage, Behördenzugriffe, Wirksamkeit der Garantien.
Pseudonymisierung	Der Personenbezug wird durch Kennungen ersetzt, sodass eine Zuordnung nur mit zusätzlichem Wissen möglich ist.
BSIG	Das deutsche BSI-Gesetz — setzt die NIS2-Richtlinie in nationales Recht um und regelt, wer betroffen ist und welche Pflichten gelten.
Least Privilege	Grundsatz der minimalen Rechte: Jede Person und jedes System erhält nur die Zugriffe, die für die Aufgabe nötig sind.
Secret-Store	Gesicherter Ablageort für Zugangsschlüssel und Passwörter — nicht im Klartext in Dateien oder im Quellcode.
Tenant Isolation (Mandantentrennung)	Technische Trennung Ihrer Daten von denen anderer Kunden beim selben Anbieter.
tamper-evident	Manipulationserkennend: Eine nachträgliche Änderung wird sichtbar, aber nicht technisch verhindert (das wäre tamper-proof).
CAPA	Korrektur- und Vorbeugemaßnahmen nach einem Vorfall: was sofort behoben wird und was die Wiederholung verhindert.
RCA (Root-Cause-Analyse)	Ursachenanalyse — die eigentliche Ursache eines Vorfalls statt nur des sichtbaren Symptoms.
Golden Tests / Golden Set	Ein fester Satz Testfälle mit erwarteten Ergebnissen, gegen den vor und nach jeder Änderung geprüft wird.
RAG	Verfahren, bei dem die KI vor der Antwort in hinterlegten eigenen Dokumenten nachschlägt, statt nur aus dem Modellwissen zu antworten.
Pinning (Modell-Version)	Eine bestimmte Modell-Version festhalten, damit ein stilles Anbieter-Update das Verhalten nicht unbemerkt ändert.
Shadow / Canary	Gestaffelter Rollout: Die neue Version läuft erst unsichtbar mit (Shadow) oder nur für einen kleinen Teil der Nutzung (Canary).
Adversarial-Tests	Gezielte Belastungstests mit ungewöhnlichen oder böswilligen Eingaben — hält das System stand?
eID	Elektronische Identität mit geprüfter Personenbindung (z. B. Ausweisfunktion) — Voraussetzung für eine rechtsverbindliche digitale Unterschrift.
AHP (Analytic Hierarchy Process)	Anerkanntes Verfahren, um Optionen anhand gewichteter Kriterien strukturiert zu bewerten und zu vergleichen.
TCO (Total Cost of Ownership)	Gesamtkosten einer Option über die Nutzungsdauer (im Werkzeug nur qualitativ, keine Euro-Zahlen).
MFA (Multi-Faktor-Authentifizierung)	Anmeldung mit einem zweiten Faktor zusätzlich zum Passwort.
TLS	Verschlüsselung der Datenübertragung (Transport Layer Security; schützt Daten in Transit).
SLA (Service-Level-Agreement)	Vertraglich zugesicherte Dienstgüte, z. B. Verfügbarkeit und Reaktionszeit.
NIS2	EU-Richtlinie zur Cyber-Sicherheit für bestimmte Unternehmen und Sektoren.
ISO/IEC 27001	Internationaler Standard für Informationssicherheits-Managementsysteme.
ISO/IEC 42001	Internationaler Standard für KI-Managementsysteme.

BEGRIFF	BEDEUTUNG
COBIT	Rahmenwerk für IT-Governance; die Routinen verweisen als Fachreferenz auf COBIT-Kontrollziele (z. B. APO13, MEA03, BAI06, DSS02).

Aufgeführt sind die Begriffe, die in diesem Bericht vorkommen; das vollständige Verzeichnis steht im User Guide.

A11

Geltungsbereich & Haftungsausschluss

Validierter Anwendungsrahmen: KMU/Mittelstand (DACH) mit niedriger bis mittlerer Regulatorik. Nicht für Banken, regulierte Finanzinstitute oder hochregulierte Hochrisiko-Systeme.

Dieser Decision Record wurde mit dem ToJo Navigator auf Basis der eingegebenen Angaben erstellt. Er stellt eine strukturierte Entscheidungs- und Dokumentationsgrundlage dar und ersetzt keine rechtliche, datenschutzrechtliche oder sicherheitstechnische Prüfung und keine Zertifizierung (z. B. nach ISO/IEC 42001 oder 27001). Verträge, Auftragsverarbeitung (AVV), Datenschutz-Folgenabschätzung (DSFA) und Anbieterangaben sind gesondert zu prüfen. Die Empfehlung gilt vorbehaltlich der internen Validierung der zugrunde liegenden Annahmen.

Erzeugt mit dem ToJo Navigator · Datum 22.09.2026 · Version 1.