Checkliste Schatten-KI im Haus v1.0
Bestandsaufnahme, Pflichten, Sofortregel und Übergang in eine freigegebene KI-Umgebung

Zur Bestandsaufnahme und Entscheidung, bevor ein KI-Dienst freigegeben wird

Fassung	v1.0 vom 10. November 2026
Geltungsbereich	katholische und evangelische Einrichtungen, Leitungsebene und Träger
Rechtsstand der zitierten Vorschriften	am 7. November 2026 an der Primärquelle geprüft, siehe Teil D
Verfasser	Nils Peters, kirchliche-ki.de
Verwendung	frei verwendbar, anpassbar und weitergebbar, mit Quellenangabe

Hinweis zur Rechtsdienstleistung. Diese Checkliste ist ein Arbeitsmittel für typische Sachverhalte und ersetzt keine Prüfung des Einzelfalls. Sie enthält keine rechtliche Würdigung für eine bestimmte Einrichtung und keine Aussage über einen bestimmten Anbieter. Die Anpassung an die konkrete Einrichtung, die rechtliche Bewertung und die Freigabe gehören zur oder zum betrieblichen Datenschutzbeauftragten beziehungsweise zur anwaltlichen Beratung der Einrichtung.

Teil A: Anwendungshinweise

Wozu diese Checkliste dient

In vielen Einrichtungen wird KI genutzt, ohne dass sie je eingeführt wurde: über private Konten bei KI-Diensten oder über KI-Assistenten, die in der Bürosoftware schon eingeschaltet sind. Verantwortlich bleibt trotzdem die Einrichtung. Diese Checkliste führt in vier Schritten von der Bestandsaufnahme zu einer freigegebenen Umgebung:

1. **Bestandsaufnahme:** Was wird im Haus tatsächlich genutzt, mit welchen Daten?
2. **Pflichten der Leitung:** Was ist geregelt, was fehlt?
3. **Sofortregel:** Was gilt, bis entschieden ist?
4. **Übergang:** Welche Umgebung taugt für die Daten, die hineinsollen?

Die Bestandsaufnahme in Schritt 1 ist zugleich die Grundlage für die Antwort auf die gemeinsame Pflichterhebung der katholischen Datenschutzaufsichten zum KI-Einsatz, die im Oktober 2026 begonnen hat.

So wird die Checkliste benutzt

- Gemeinsam mit der oder dem betrieblichen Datenschutzbeauftragten durchgehen, bei Schritt 2 und 4 möglichst auch mit der Mitarbeitervertretung.
- Jede Antwort "nein" oder "offen" ist ein Arbeitsauftrag. Teil C ordnet sie.
- Die ausgefüllte Checkliste datiert ablegen. Beide Kirchengesetze verlangen, dass die Einrichtung die Einhaltung der Grundsätze nachweisen kann (§ 7 Abs. 2 KDG; § 5 Abs. 2 DSG-EKD).

Was diese Checkliste nicht leistet

Sie ersetzt weder die Datenschutz-Folgenabschätzung noch die Risikoanalyse, sondern liefert ihnen die Tatsachen. Sie bewertet keinen Anbieter. Für die Fragen an einen Anbieter zur Verarbeitungskette gibt es einen eigenen Fragebogen auf kirchliche-ki.de.

Teil B: Fragen

Schritt 1: Bestandsaufnahme

1.1	Ist bekannt, welche KI-Dienste Beschäftigte dienstlich nutzen, einschließlich privater Konten? Eine anonyme Umfrage liefert ehrlichere Antworten als eine Anordnung.	☐ ja ☐ nein ☐ offen	§ 7 Abs. 2 KDG; § 5 Abs. 2 DSG-EKD
1.2	Ist geprüft, welche KI-Funktionen in der vorhandenen Bürosoftware enthalten und eingeschaltet sind?	☐ ja ☐ nein ☐ offen	§ 26 Abs. 1 KDG; § 27 Abs. 1 DSG-EKD
1.3	Falls solche Funktionen eingeschaltet sind: Ist dokumentiert, wer das entschieden hat?	☐ ja ☐ nein ☐ offen	§ 7 Abs. 2 KDG; § 5 Abs. 2 DSG-EKD
1.4	Ist bekannt, ob diese Funktionen Daten an Dienste senden, die nicht vom Auftragsverarbeitungsvertrag erfasst sind, etwa eine Websuche?	☐ ja ☐ nein ☐ offen	§ 29 KDG; § 30 DSG-EKD
1.5	Ist bekannt, welche Arten von Daten in KI-Dienste eingegeben werden: Gesundheits-, Sozial- oder Personaldaten, Inhalte aus der Seelsorge?	☐ ja ☐ nein ☐ offen	§§ 9, 13, 14 KDG-DVO; § 27 DSG-EKD
1.6	Katholisch: Ist geklärt, ob die Einrichtung zur Pflichterhebung der Aufsichten aufgefordert ist? Ist die Antwort vorbereitet?	☐ ja ☐ nein ☐ offen	§ 46 Buchst. b KDG

Schritt 2: Pflichten der Leitung

2.1	Gibt es eine schriftliche Regel zur Nutzung von KI-Diensten (Dienstanweisung, Richtlinie oder Dienstvereinbarung)?	☐ ja ☐ nein ☐ offen	§ 26 Abs. 5 KDG; § 27 Abs. 5 DSG-EKD
2.2	Gibt es für jeden genutzten KI-Dienst einen Vertrag zur Auftragsverarbeitung?	☐ ja ☐ nein ☐ offen	§ 29 Abs. 3 KDG; § 30 Abs. 3 DSG-EKD
2.3	Sind die genutzten Dienste eingeordnet, nach katholischem Recht in eine Datenschutzklasse, nach evangelischem Recht nach ihrem Risiko? Fehlt die Einordnung, gilt nach katholischem Recht automatisch Klasse III.	☐ ja ☐ nein ☐ offen	§ 9 Abs. 5 KDG-DVO; § 27 Abs. 1 DSG-EKD
2.4	Ist geprüft, ob eine Datenschutz-Folgenabschätzung nötig ist? Ist dazu der Rat der oder des Datenschutzbeauftragten eingeholt?	☐ ja ☐ nein ☐ offen	§ 35 Abs. 1 und 2 KDG; § 34 DSG-EKD
2.5	Ist die Mitarbeitervertretung beteiligt oder ihre Beteiligung geprüft? Nach beiden Rechten genügt, dass der Dienst objektiv zur Überwachung von Verhalten oder Leistung geeignet ist. Katholisch kommt die Anhörung bei grundlegender Änderung der Arbeitsmethoden hinzu.	☐ ja ☐ nein ☐ offen	§ 40 Buchst. k MVG-EKD; § 36 Abs. 1 Nr. 9 und § 29 Abs. 1 Nr. 14 MAVO
2.6	Wird die KI-Kompetenz der Beschäftigten unterstützt, an den Werkzeugen, die tatsächlich freigegeben sind?	☐ ja ☐ nein ☐ offen	Art. 4 KI-VO

Schritt 3: Sofortregel

3.1	Wissen alle Beschäftigten, welche Daten bis zur Klärung in keinen KI-Dienst gehören?	☐ ja ☐ nein ☐ offen	§ 26 Abs. 5 KDG; § 27 Abs. 5 DSG-EKD
3.2	Ist die Verwendung privater Konten für dienstliche Daten ausdrücklich ausgeschlossen?	☐ ja ☐ nein ☐ offen	DSK-Orientierungshilfe KI, Rn. 41
3.3	Ist benannt, an wen sich Beschäftigte mit Fragen zur KI-Nutzung wenden?	☐ ja ☐ nein ☐ offen	
3.4	Ist geregelt, was geschieht, wenn personenbezogene Daten in einen nicht freigegebenen Dienst gelangt sind (interne Meldung, Prüfung der Meldepflicht)?	☐ ja ☐ nein ☐ offen	§ 33 KDG (unverzüglich, nach 72 Stunden mit Begründung); § 32 DSG-EKD (unverzüglich)
3.5	Sind KI-Funktionen der Bürosoftware, über die nicht entschieden ist, bis zur Entscheidung abgeschaltet oder in ihrer Nutzung begrenzt?	☐ ja ☐ nein ☐ offen	§ 26 Abs. 1 KDG; § 27 Abs. 1 DSG-EKD

Schritt 4: Übergang in eine freigegebene Umgebung

Ausgangspunkt sind die Daten aus 1.5, nicht das Werkzeug, das schon da ist.

4.1	Gibt es eine freigegebene KI-Umgebung, die für die tatsächlich eingegebenen Daten taugt, sodass niemand auf private Konten ausweichen muss?	☐ ja ☐ nein ☐ offen	KDSZ Dortmund, Jahresbericht 2025, 2.5.3
4.2	Besteht ein Vertrag zur Auftragsverarbeitung nach kirchlichem Recht?	☐ ja ☐ nein ☐ offen	§ 29 KDG; § 30 DSG-EKD
4.3	Ist vertraglich ausgeschlossen, dass Eingaben für eigene Zwecke des Anbieters verwendet werden, auch nicht zum Training?	☐ ja ☐ nein ☐ offen	§ 29 Abs. 3 KDG; § 30 Abs. 1 DSG-EKD
4.4	Ist bekannt, wo jede Anfrage verarbeitet wird, nicht nur, wo die Daten liegen?	☐ ja ☐ nein ☐ offen	Fragebogen Verarbeitungskette, kirchliche-ki.de
4.5	Ist ab Werk keine Funktion eingeschaltet, über die Daten das Haus verlassen? Ist jede solche Funktion vom Vertrag erfasst?	☐ ja ☐ nein ☐ offen	§ 29 KDG; § 30 DSG-EKD
4.6	Bestimmt das Haus selbst, welche Modelle und Funktionen eingeschaltet sind? Kommen neue Funktionen nicht ungefragt hinzu?	☐ ja ☐ nein ☐ offen	§ 26 Abs. 1 KDG; § 27 Abs. 1 DSG-EKD
4.7	Ist ein Wechsel des Anbieters möglich, mit einer Exit-Strategie vor Beginn der Nutzung? Lassen sich Verläufe und Dokumente mitnehmen oder nachweisbar löschen?	☐ ja ☐ nein ☐ offen	§ 18 Abs. 2 Buchst. d und Abs. 3 KDG-DVO
4.8	Katholisch: Ist die Umgebung bereits geprüft und freigegeben, etwa durch die Leitungsebene für ihre Träger?	☐ ja ☐ nein ☐ offen	§ 18 Abs. 1 KDG-DVO
4.9	Läuft der Zugang über dienstliche Konten? Ist geregelt, wer welche Verläufe sehen und auswerten darf?	☐ ja ☐ nein ☐ offen	§ 38 Abs. 1 Nr. 11 MAVO; § 40 Buchst. k MVG-EKD
4.10	Passt die Umgebung zur Datenschutzklasse oder Risikostufe der Daten, die hineinsollen? Für Inhalte aus der Seelsorge gilt ein Schutzniveau oberhalb der Klasse III.	☐ ja ☐ nein ☐ offen	§§ 13, 14 KDG-DVO; § 27 DSG-EKD
4.11	Erfolgt die Freigabe zusammen mit einer Schulung an genau dieser Umgebung?	☐ ja ☐ nein ☐ offen	Art. 4 KI-VO

Teil C: Auswertung

Offen in Schritt 1	Zuerst klären. Ohne Bestandsaufnahme lässt sich weder die Pflichterhebung beantworten noch eine Umgebung auswählen.
Nein in Schritt 3	Sofort handeln. Eine kurze Anweisung schließt die größten Lücken schnell.
Nein in Schritt 2	Pflichten nachholen, mit Datenschutzbeauftragten und Mitarbeitervertretung. Die fehlende Regel ist der häufigste Befund.
Nein in Schritt 4 bei Gesundheits-, Sozial- oder Personaldaten	Die Umgebung ist für diese Daten nicht freigabefähig. Entweder die Umgebung wechseln oder die Daten ausdrücklich ausschließen. Ein Ausschluss allein bringt die Nutzung erfahrungsgemäß zurück in den Schatten.

Teil D: Quellen

- **KDG**, Lesefassung in der Fassung des Beschlusses vom 24. November 2025, Anlage zum Amtsblatt des Erzbistums Berlin 03/2026.
- **KDG-DVO** in der Fassung des Beschlusses vom 24. November 2025 (§§ 9, 13, 14, 18). Inkraftsetzung beider Änderungen je Bistum.
- **Rahmen-MAVO**, Stand 1. Februar 2023. Diözesane Fassungen können abweichen. Zu § 36 Abs. 1 Nr. 9: Kirchlicher Arbeitsgerichtshof, Urteil vom 15. Mai 2020, M 20/2019, Rn. 22.
- **DSG-EKD**, Neufassung vom 15. Januar 2025 (ABl. EKD S. 1).
- **MVG-EKD**, Neufassung vom 20. Januar 2024, Stand 18. Februar 2026.
- **Verordnung (EU) 2024/1689** (KI-Verordnung), Art. 4 in der Fassung der Verordnung (EU) 2026/1744.
- **DSK**, Orientierungshilfe "Künstliche Intelligenz und Datenschutz", Version 1.0 vom 6. Mai 2024, Rn. 36 und 41.
- **Katholisches Datenschutzzentrum Dortmund**, Jahresbericht 2025, Abschnitt 2.5.3, sowie Meldung zur gemeinsamen Erhebung zum KI-Einsatz vom 21. Oktober 2026.

Die Begründung zu dieser Checkliste steht in der Ausgabe "Die KI ist schon im Haus. Wer hat das beschlossen?" auf kirchliche-ki.de.