

KI im Unterricht: Was geht – und was nicht? / KI-Verordnung

Orientierungshilfe für Lehrkräfte – verdichtet aus DSK, KMK, EDPB, AI Act und Praxisanalyse

Die gute Nachricht vorweg: KI-Nutzung im Unterricht ist kein „Dienstvergehen“ – wenn man die richtigen Wege wählt. Die rechtliche Lage ist komplex (DSGVO, AI Act, Landesrecht), aber aus der Schnittmenge aller Vorgaben lassen sich klare, praktikable Regeln ableiten: was sicher nutzbar ist, was Vorsicht erfordert und wovon abzuraten ist.

Fünf Guardrails, die immer gelten

Diese fünf Regeln leiten sich direkt aus DSK-Orientierungshilfe, EDPB-Empfehlungen und Art. 4 KI-VO ab:

- Keine personenbezogenen Daten in Prompts.** Weder Schülernamen, Notenlisten, Gesundheitsdaten noch identifizierende Details. Auch nicht „testweise“. Aufgaben mit fiktiven Daten oder anonymisierten Texten konstruieren.
- Keine Leistungsbewertung durch KI.** Ab August 2026 gelten KI-Systeme zur Bewertung von Lernergebnissen als Hochrisiko-Systeme (AI Act). Die pädagogische Bewertungshoheit bleibt bei der Lehrkraft. KI als Feedback-Impuls: ja. KI als Notengeberin: nein.
- Nur freigegebene Systeme für aktive Schülernutzung.** Landeslösungen oder Dienste mit Auftragsverarbeitungsvertrag (AVV). Eigene Consumer-Accounts (ChatGPT, Gemini) sind für Schülernutzung nicht geeignet.
- Transparenz gegenüber Lernenden und Eltern.** Über den Einsatz informieren, Zweck benennen, auf Rechte hinweisen (Auskunft, Löschung, Widerspruch). Dokumentation im Verarbeitungsverzeichnis.
- KI-Kompetenz ist Pflicht, nicht Kür.** Seit Februar 2025 verpflichtet Art. 4 KI-VO Schulen als Betreiber, für ausreichende KI-Kompetenz bei Lehrkräften und Lernenden zu sorgen. Fortbildung ist damit Compliance – nicht nur Didaktik.

Zugangsweg-Bewertung: Die Ampeltabelle

Bewertungslogik: Nicht der Tool-Name entscheidet, sondern ob AVV vorhanden, Drittlandtransfer geregelt, Training-Opt-out dokumentiert und keine personenbezogenen Daten übermittelt werden.

Zugangsweg	Ampel	Begründung / Bedingung	Geeignet für
Landeslösungen (F13, telli, ByLKI)	GRÜN	Datenschutz liegt beim Land als Verantwortlichem. Kein individuelles Haftungsrisiko für Lehrkräfte. AVV und DSFA auf Landesebene geregelt.	Alle – Lehrkräfte und Schüler
Lokale Modelle (Ollama, LM Studio)	GRÜN	Kein Drittlandtransfer, kein externer Processor. Maximale Datensouveränität. Voraussetzung: Schule/Träger betreibt und wartet die Infrastruktur.	Informatik-Unterricht, Projekte, Lehrkraft-Vorbereitung
Mistral API (über schulisches Frontend)	GELB–GRÜN	EU-Unternehmen, EU-Hosting, DPA verfügbar. Starke DSGVO-Position. Aber: Opt-out für Training aktiv sicherstellen und dokumentieren. Kommerzieller Account mit DPA erforderlich.	Lehrkräfte; Schüler nur über schuleigenes Frontend mit dokumentiertem Opt-out
Edu-Plattformen mit AVV (fobizz, SchulKI, FelloFish)	GELB	AVV vorhanden, anonymisierte Nutzung möglich. Aber: Inferenz teils auf US-Infrastruktur. Datenminimierung konsequent einhalten. Upload von Schülerarbeiten kritisch prüfen.	Schülernutzung möglich, wenn AVV vorliegt und keine personenbezogenen Daten eingegeben werden
Anonyme Proxies (xPrivo, Duck.ai, Brave Ask)	GELB	Privacy by Design, keine Accounts, lokale Speicherung. Gutes Risikoprofil. Aber: kein schulisch gestaltbarer AVV, keine Weisungsbindung. Für Demonstration und Recherche gut geeignet, wenn keine personenbezogenen Daten eingegeben werden.	Lehrkraft-Recherche, angeleitete Demonstration, Medienkompetenz-Übungen
DeepInfra (als Schüler-Tool)	GELB-ROT	Bei vollständig anonymisiertem Zugang (kein Personenbezug) pragmatisch denkbar, aber institutionell nicht abgesichert. US-Hosting, Debug-Sampling vorbehalten.	Nur persönliche Lehrkraft-Nutzung ohne Schülerdaten
Consumer-LLM (ChatGPT, Gemini, Claude)	ROT	Kein AVV, kein Opt-out garantiert, US-Hosting, Profilbildung. Für Schülernutzung im Unterricht nicht geeignet. Lehrkraft-eigene Vorbereitung ist tolerierbar.	Nur persönliche Lehrkraft-Nutzung ohne Schülerdaten
OpenRouter / (als Schüler-Tool)	ROT	OpenRouter: weitgehende Lizenz bei aktiviertem Logging, intransparente Sub-Prozessorkette. Für schulische Schülernutzung nicht vertretbar.	Nicht für Schüler. Für Lehrkraft nur mit Vorsicht

Der Silberstreifen am Horizont

Lehrkräfte stehen nicht vor einer Wand, sondern vor einer Tür mit Schloss. Der Schlüssel ist die richtige Kombination aus Zugangsweg und Nutzungsregel:

Für den Alltag: Landeslösungen nutzen (auch wenn die Modellqualität nicht immer überzeugt) – hier ist die Haftung institutionell abgesichert. Parallel Edu-Plattformen mit AVV einsetzen, wenn die Landeslösung nicht ausreicht.

Für ambitionierte Projekte: Mistral API mit schulischem Frontend oder lokale Modelle via Ollama. Beides ist DSGVO-nah, erfordert aber technische Kompetenz und Dokumentation.

Für schnelle Recherche/Demo: xPrivo oder Duck.ai – ohne personenbezogene Daten in Prompts. Ideal für angeleitete Medienkompetenz-Übungen.

Entscheidend ist nicht das perfekte Tool, sondern die konsequente Einhaltung der fünf Guardrails.

Klare No-Gos

Schüler mit privaten Accounts bei US-Anbietern arbeiten lassen (ChatGPT, Gemini, Claude Consumer).

Personenbezogene Daten (Namen, Noten, Förderpläne, Gesundheitsdaten) in beliebige KI-Prompts eingeben.

KI-Systeme zur autonomen Leistungsbewertung oder Prüfungsüberwachung einsetzen.

Tools ohne AVV für aktive Schülernutzung freigeben – auch nicht „nur kurz“ oder „nur zum Testen“.

Hinweis für die Fortbildungspraxis

Art. 4 KI-VO verpflichtet Schulen seit Februar 2025 zur Sicherstellung von KI-Kompetenz. **Diese Fortbildung ist daher nicht nur didaktisch sinnvoll, sondern Teil der institutionellen Compliance.** Lehrkräfte, die an KI-Fortbildungen teilnehmen, handeln im Sinne der Verordnung – und reduzieren gleichzeitig ihr individuelles Haftungsrisiko.

Quellengrundlage

Dieses Dokument verdichtet Ergebnisse aus: DSK-Orientierungshilfe KI und Datenschutz (2024), KMK-Handlungsempfehlung KI (10/2024), EDPB-Empfehlungen zu Transfermechanismen, EU KI-Verordnung 2024/1689, VIDIS-Prüfkriterien V0.2, Mistral AI DPA (03/2026), sowie aus unabhängigen Analysen der Datenschutz- und Nutzungsbedingungen von fobizz, FelloFish, SchulKI, OpenRouter, DeepInfra, xPrivo, Duck.ai und Brave Ask.

Rechtshinweis: Dieses Dokument ersetzt keine Rechtsberatung. Es dient der praxisnahen Orientierung für Lehrkräfte und KI-Fortbildner. Die rechtliche Bewertung einzelner Tools kann sich durch Vertragsänderungen der Anbieter oder neue Aufsichtsbehörden-Entscheidungen jederzeit verschieben.

Art. 4 KI-Verordnung – KI-Kompetenz ist Pflicht

Was steht in Art. 4?

Seit dem 2. Februar 2025 verpflichtet die europäische KI-Verordnung (EU 2024/1689) **alle Betreiber von KI-Systemen** – ausdrücklich auch Schulen – dafür zu sorgen, dass ihr Personal über ein **ausreichendes Maß an KI-Kompetenz** verfügt (Art. 4 Abs. 1). Die Pflicht gilt **risikoklassenunabhängig**: Sie greift bei ChatGPT und telli genauso wie bei fobizz oder selbst gehosteten Modellen. Gefordert wird kein Expertenwissen, sondern ein kontextangemessenes Verständnis von Funktionsweise, Grenzen und Risiken.

Was muss konkret geschult werden?

Art. 3 Nr. 56 KI-VO definiert KI-Kompetenz als Fähigkeit, KI-Systeme *informiert einzusetzen und sich ihrer Risiken bewusst zu sein*. Für den schulischen Kontext lassen sich drei Säulen ableiten:

Säule	Was Lehrkräfte wissen bzw. können müssen
Technisches Grundverständnis	Was ist ein Sprachmodell (LLM)? Warum erzeugt es plausibel klingende, aber falsche Antworten (Halluzinationen)? Wo liegen die systematischen Grenzen generativer KI?
Datenschutz-Awareness	Welche Daten dürfen in Prompts eingegeben werden, welche nicht? Was regelt ein Auftragsverarbeitungsvertrag (AVV)? Wie unterscheiden sich Landeslösungen von Consumer-Accounts?
Risikobewusstsein	Wann wird ein KI-System zum Hochrisiko-System (z. B. Leistungsbewertung, Proctoring)? Was sind verbotene Praktiken (z. B. Emotionserkennung)? Wo liegt die Grenze zwischen Feedback-Tool und Bewertungsinstrument?

Hinzu kommt die **kontextbezogene Handlungskompetenz**: Lehrkräfte müssen datenschutzkonforme Aufgabenstellungen konstruieren und den KI-Einsatz im Unterricht nachvollziehbar dokumentieren können.

Warum betrifft das Lehrkräfte direkt?

Schulen gelten als **Betreiber** im Sinne der KI-VO, sobald sie KI-Systeme im Unterricht oder in der Verwaltung einsetzen. Die Kompetenzpflicht ist damit **kein Appell, sondern geltendes EU-Recht**. Fortbildung wird zur Compliance-Maßnahme. Laut Hinweisen der Bundesakademie für öffentliche Verwaltung (BAköV) reicht das bloße Lesen einer Produkthanleitung dabei ausdrücklich **nicht** aus.

Was droht bei Nicht-Einhaltung?

Die KI-VO sieht Sanktionen von bis zu **15 Mio. € bzw. 3 % des Jahresumsatzes** vor. Adressat ist der Betreiber (Schulträger/Land), nicht die einzelne Lehrkraft. Gleichwohl gilt: Wer an einer qualifizierten Fortbildung teilnimmt, handelt nachweislich im Sinne der Verordnung und **reduziert das eigene Haftungsrisiko** erheblich.

✓ Diese Fortbildung erfüllt die Anforderungen nach Art. 4 KI-VO

Die Teilnahme an dieser KI-Fortbildung vermittelt die in Art. 4 geforderte KI-Kompetenz und ist dokumentierbar. Damit leisten Sie einen nachweisbaren Beitrag zur Compliance Ihrer Schule im Sinne der europäischen KI-Verordnung.

Quellen: Art. 4 KI-VO (EU 2024/1689) · Art. 3 Nr. 56 KI-VO · EU AI Office FAQ zu AI Literacy · BMI/BAköV-Hinweise zum Kompetenzaufbau