DATENSCHUTZ & DSGVO BEI KI-TOOLS

Ein Leitfaden für rechtssicheren KI-Einsatz an Schulen

KI-AKADEMIE FÜR LEHRKRÄFTE
by educaite

Material der KI-Akademie für Lehrkräfte von educaite

> **Hinweis:** *Dieses Infosheet ersetzt keine Rechtsberatung. Es fasst den aktuellen Stand allgemein verständlich zusammen. Im konkreten Einzelfall wenden Sie sich bitte an Ihre/n schulische/n Datenschutzbeauftragte/n oder eine/n Fachjurist/in.*

Mit dem flächendeckenden Einsatz von KI-Tools im Unterricht ist Datenschutz vom Spezialthema zur Alltagsfrage geworden. Wer *ChatGPT*, *Gemini* oder *Copilot* mit Schülerdaten füttert, verlässt schnell den rechtssicheren Rahmen.

⚠ Häufige Stolperfallen im Schulalltag

1. **Klassenarbeiten in der KI:** Texte mit Schülernamen werden zur Korrektur hochgeladen. Auch wenn es Zeit spart – das ist eine unzulässige Datenübermittlung.
2. **Notizen & Elterngespräche:** Pädagogische Vermerke werden zur „Strukturierung" in einen Chatbot eingegeben. Diese Inhalte zählen als Diensttdaten, nicht als private Notizen.
3. **„Kostenlos" ist nicht rechtssicher:** Free-Tier-Tools haben in der Regel keinen Auftragsverarbeitungsvertrag (AVV) und nutzen Eingaben oft zum Training.

Die rechtlichen Grundlagen kompakt

1. Was sind personenbezogene Daten?

Mehr als nur Namen: Auch Klassenfotos, Notenstände, Verhaltensauffälligkeiten, Lernstandsdiagnosen oder Sprachaufnahmen sind personenbezogen. Bereits ein Vorname plus Klassenangabe („Lukas, 7b, Gymnasium Musterstadt") genügt für eine Re-Identifizierung. Wenn Sie aus dem Kontext einen Schüler wiedererkennen, kann es ein Gericht auch.

2. Schülerdaten in KI-Eingaben

- **Goldene Regel:** Niemals Klarnamen, Klassenarbeiten oder Zeugnisse in öffentliche Chatbots eingeben – auch nicht „nur kurz zur Probe".
- **Anonymisierung vor dem Prompt:** Namen durch „Schüler A" ersetzen, Schul- und Ortsbezug entfernen, eindeutige Stilmerkmale prüfen.

- **Auch privater Account = Diensttdaten:** Das schulische Datenschutzrecht gilt unabhängig vom genutzten KI-Konto.
- **Sprachaufnahmen sind besonders sensibel:** Stimme zählt als biometrisches Merkmal.

3. Auftragsverarbeitung & US-Anbieter

Ohne Auftragsverarbeitungsvertrag (Art. 28 DSGVO) ist die Nutzung im dienstlichen Kontext rechtswidrig – auch bei „kostenlosen" Tools. Das EU-USA Data Privacy Framework erlaubt seit 2023 Datenübertragungen in die USA, aber nur an zertifizierte Anbieter. Achten Sie auf *Education*- oder *Enterprise*-Pakete; Privat-Accounts haben in der Regel keinen AVV.

4. Einwilligung & elterliche Zustimmung

- **Altersgrenze:** Unter 16 Jahren ist die Einwilligung der Erziehungsberechtigten nötig – manche Bundesländer ziehen die Grenze bei 14 oder 18.
- **Drei Kriterien:** Die Einwilligung muss freiwillig, informiert und widerruflich sein. Keine Notenrelevanz, keine Gruppendynamik-Pflicht.
- **Alternative anbieten:** Wer nicht einwilligt, erhält eine gleichwertige Aufgabe ohne KI-Nutzung.

KI-Tools rechtssicher auswählen

1. Verarbeitungsort prüfen

EU-Hosting bevorzugen – Tools mit Rechenzentren in Deutschland oder EU-Staaten (z. B. Aleph Alpha, Mistral) reduzieren rechtliche Risiken erheblich.

2. AVV vor dem ersten Einsatz

Der AVV wird vom Schulträger oder der Schulleitung unterschrieben – nicht von einzelnen Lehrkräften. Die Datenschutzbeauftragten der Länder bieten mittlerweile Musterverträge für die gängigen KI-Anbieter an.

3. Trainingsdaten-Klausel beachten

Frage Nr. 1 an jeden Anbieter: „Werden meine Eingaben zum Training genutzt?" Wenn ja: nicht im Schulkontext einsetzen. Viele Tools erlauben in den Einstellungen das Abschalten der Trainings-Verwendung – diese Einstellung gehört zur Inbetriebnahme dazu.

4. Bildungslizenzen nutzen

- **Schul-Pakete:** Microsoft (Copilot Education) und Google (Gemini for Education) bieten DSGVO-konforme Pakete – oft mit AVV inklusive.
- **Landeslizenzen:** Mehrere Bundesländer haben 2025/2026 landesweite Rahmenverträge geschlossen. Erkundigen Sie sich beim Schulträger.

✓ Best Practice: Die Drei-Sekunden-Prüfung

Bevor Sie einen Prompt absenden, stellen Sie sich drei Fragen:

1. **Personenbezogen?** Stehen im Text Namen, Klassen, Schule, Geburtsdatum oder eindeutige Stilmerkmale?
2. **Anonymisierbar?** Lassen sich diese Bezüge entfernen, ohne den Prompt sinnlos zu machen?
3. **Tool freigegeben?** Hat das Tool einen AVV mit Ihrer Schule?

Dreimal „Ja" → loslegen. Einmal „Nein" → Stopp und eine Alternative wählen.

Fazit

Datenschutz ist keine Innovationsbremse, sondern Voraussetzung für nachhaltiges Vertrauen in KI im Klassenzimmer. Mit klaren Routinen – Anonymisierung vor dem Prompt, AVV vor dem Einsatz, Bildungslizenz statt Privat-Account – lassen sich rund 90 % aller Risiken im Alltag vermeiden, ohne dass pädagogische Möglichkeiten geopfert werden.