

# 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

## DAS WICHTIGSTE AUF EINER SEITE

**Datenschutz heißt nicht „KI ist verboten“.** Er heißt: bewusst entscheiden und sauber organisieren. Eine einzige Regel verhindert die meisten Probleme – keine personenbezogenen Daten in offene KI-Tools. Diese Seite genügt für den Alltag, die Details und der rechtliche Rahmen folgen ab Seite 2.

## DIE KERNREGELN AUF EINEN BLICK

### ① Goldene Regel

Keine Klarnamen, Noten, Förderpläne oder Beobachtungen einzelner Schüler:innen eingeben. **(DSGVO!)**

### ② Datenminimierung

Nur das Nötige: Thema, Stufe, Kompetenzziel, Zeitumfang. Mehr braucht die KI nicht.

### ③ Richtig anonymisieren

„Max“ durch „Schüler:in“ zu ersetzen reicht nicht – auch Merkmalskombinationen können identifizieren.

### ✓ Unbedenklich (anonym)

- Stunden & Arbeitsblätter generieren
- Texte vereinfachen / differenzieren
- Allgemeine Feedback-Bausteine

### ④ Tool-Kategorie wählen

Lokal/offline > schulisch freigegeben > offener Webdienst (höchste Vorsicht).

### ⑤ Assistenz, kein Autopilot

KI-Ausgaben prüfen und anpassen. Die Verantwortung bleibt bei Ihnen und der Schule.

### ⑥ Zwei Rechtsrahmen

DSGVO *und* EU AI Act. Notengebung/Prüfungsüberwachung per KI gelten als hochriskant.

### ✗ Nicht ins Tool geben

- Namen, Geburtsdaten, Notenlisten
- Individuelle Förderpläne / Diagnosen
- Komplette Schülertexte mit Namenskopf

## SO FORMULIERT MAN ES DATENSPARSAM

Statt „Förderhinweis für Max Mustermann, 7b, LRS, Note 5“ → „Formuliere allgemeine Förderhinweise für Lernende mit LRS in Klasse 7, Schwerpunkt Rechtschreibung: Motivation, kurze Übungen, Feedback-Sätze.“

**Hinweis:** Dieses Infosheet ersetzt keine Rechtsberatung. Es fasst den Stand 2026 allgemein verständlich zusammen. Maßgeblich sind die Vorgaben Ihres Bundeslandes und Schulträgers; im Einzelfall wenden Sie sich an Ihre/n Datenschutzbeauftragte/n oder eine/n Fachjurist/in.

## Die zwei Rechtsrahmen verstehen

Beim KI-Einsatz greifen 2026 zwei Regelwerke ineinander. Sie müssen kein Jurist sein – aber die Grundlogik hilft, sicher zu entscheiden.

### 1. DSGVO – Schutz personenbezogener Daten

Die Datenschutz-Grundverordnung schützt alle Daten, die sich auf eine identifizierbare Person beziehen: Namen, Noten, Förderbedarfe, Verhaltensbeobachtungen, Gesundheitsangaben. Viele KI-Tools laufen als Cloud-Dienste – eingegebene Inhalte können an externe Anbieter übertragen werden. Für die Verarbeitung im Auftrag der Schule braucht es in der Regel einen **Auftragsverarbeitungsvertrag (AVV)** und eine Rechtsgrundlage; bei Minderjährigen ist die Einwilligung der Erziehungsberechtigten ein sensibler Punkt.

**Im Zweifel: erst freigeben lassen, dann nutzen.**

### 2. EU AI Act – die Risiko-Logik

Die KI-Verordnung stuft Anwendungen nach Risiko ein. Als **hochriskant** gelten im Bildungsbereich u. a. KI zur Notengebung, zur Bewertung von Leistungen, zur Prüfungsüberwachung und zur Erkennung von Lernschwierigkeiten. Solche Systeme unterliegen strengen Auflagen (Transparenz, Aufsicht, Nachvollziehbarkeit). Für den Alltag wichtig: Eine generelle **KI-Kompetenzpflicht** verlangt, dass Beschäftigte im Umgang mit KI geschult sind – die Bestimmungen greifen gestaffelt bis 2026. Der bloße Einsatz eines Schreibassistenten zur eigenen Vorbereitung fällt nicht in die Hochrisiko-Klasse, das automatisierte Bewerten von Schüler:innen hingegen schon.

#### **Faustregel**

Je näher eine KI-Anwendung an einer *Entscheidung über einzelne Schüler:innen* ist (Note, Versetzung, Förderdiagnose), desto strenger die Regeln – und desto eher gehört die Entscheidung in menschliche Hand statt in ein Tool.

# Die goldene Regel: keine personenbezogenen Daten

Wenn Sie im Kollegium nur eine Regel etablieren, dann diese: **Keine personenbezogenen Daten in nicht freigegebene KI-Tools**. Keine Klarnamen, keine Geburtstage, keine Notenlisten, keine individuellen Förderpläne, keine Freitext-Beobachtungen über Einzelne.

## 1. Anonymisieren – aber richtig

„Max“ durch „Schüler:in“ zu ersetzen genügt oft nicht. Ein Text bleibt identifizierend, wenn die *Kombination* von Merkmalen eine Person wiedererkennbar macht – seltene Ereignisse, konkrete Orte, exakte Zitate, Namen im Dokumentkopf. Gute Anonymisierung heißt: keine wiedererkennbare Merkmalskombination, keine Originaltexte mit eindeutigen Kennzeichen. **(Im Zweifel lieber nur Kriterien beschreiben statt Originaltext.)**

## 2. Aus „heikel“ wird „unbedenklich“

- **Statt** „Schreibe ein Feedback für Lena K., 9c, Note 4 in der letzten Klausur“ **besser** „Formuliere 8 allgemeine Feedback-Sätze zu argumentativen Texten, Klasse 9, Niveau ausbaufähig“.
- **Statt** kompletten Aufsatz mit Namen einfügen **besser** nur die Fehlerart oder einen anonymisierten Auszug beschreiben.
- **Sensible Themen** (Gesundheit, Diagnosen, Konflikte) gar nicht erst mit öffentlicher KI bearbeiten.

# Tool-Auswahl: drei Kategorien

Nicht jedes Tool ist gleich riskant. Für die Praxis hilft eine einfache Staffelung – von sicher nach „nur mit Vorsicht“:

## 1. Lokal / offline

Läuft auf dem Schul- oder Eigengerät, ohne Daten nach außen zu senden – datenschutzseitig am unkritischsten, aber technisch (noch) selten im Alltag.

## 2. Schulisch freigegebene Dienste

Plattformen, die auf den Schuleinsatz zugeschnitten sind (z. B. fobizz, telli, SchulKI). Sie werben mit DSGVO-freundlicher Gestaltung – teils EU-Serverstandort, teils ohne eigene Schüler-Accounts, teils mit AVV für Schulträger.

**Status nach Anbieterangaben – bitte die für Ihre Schule freigegebene Liste und Ihre Datenschutzbeauftragten beachten.** Funktionsumfang und Konditionen ändern sich.

## 3. Frei zugängliche Webdienste

Allgemeine Assistenten (z. B. ChatGPT, Gemini, Claude) sind leistungsstark, aber für Schülerdaten ungeeignet. Eingaben können je nach Einstellung zur Modellverbesserung genutzt werden. Nur für die eigene Vorbereitung mit *anonymisierten* Inhalten verwenden – und Einstellungen zum Daten-Opt-out prüfen.

### Häufige Fehler

- Schülertexte komplett kopieren – besser anonymisierte Auszüge oder nur Fehlerarten beschreiben.
- Noten, Förderbedarfe, Konfliktverläufe eingeben – stattdessen allgemeine Strategien abfragen.
- KI-Ergebnis 1:1 übernehmen – immer fachlich prüfen und anpassen.
- Keine Absprache im Kollegium – führt zu unkoordinierter „Schatten-Nutzung“.

## Praxis: eine Minimal-Policy fürs Kollegium

Ein klarer Rahmen schlägt sowohl „einfach machen und hoffen“ als auch „alles verbieten“. Fünf Sätze genügen für den Start:

- Keine personenbezogenen Daten in nicht freigegebene KI-Tools.
- Schülerarbeiten nur anonymisiert und nur, wenn pädagogisch nötig.
- KI-Ausgaben werden geprüft, angepasst und als Entwurf behandelt.
- Sensible Themen (Gesundheit, Diagnosen, Konflikte) nicht mit KI bearbeiten.
- Bei Unsicherheit: erst Rückfrage an Datenschutz-/Schulleitung.

### ✓ Best Practice: Liste „freigegebene Tools“ führen

Legen Sie schulintern eine kurze, gepflegte Liste freigegebener Tools an – plus jeweils eine Alternative für Aufgaben ganz ohne personenbezogene Eingaben. Das gibt dem Kollegium Sicherheit und verhindert Wildwuchs. Ergänzen Sie das Datum der letzten Prüfung, da sich der Status von Diensten ändern kann.



### Fazit

Datenschutzkonforme KI-Nutzung ist machbar – nicht durch Perfektion, sondern durch einen pragmatischen Rahmen: Daten minimieren, anonymisieren, klare Regeln, geprüfte Ergebnisse. Wer keine personenbezogenen Daten eingibt und freigegebene Tools nutzt, ist im Schulalltag gut aufgestellt. Die rechtliche Letztverantwortung bleibt bei Schule und Träger.