

# DIE REGULIERUNG VON KÜNSTLICHER INTELLIGENZ

## Auswirkungen der geplanten KI-Verordnung auf Bildungsplattformen

Sebastian Straub, LL.M., VDI/VDE Innovation und Technik GmbH

Stand Januar 2022

Die Europäische Kommission hat einen Verordnungsentwurf zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz vorgelegt.<sup>1</sup> Die Verordnung sieht für bestimmte KI-Anwendungen im Bildungsbereich hohe Compliance-Anforderungen vor. Digitale Bildungsplattformen und Bildungsanbieter sollten sich frühzeitig mit den Auswirkungen der Verordnung auseinandersetzen. Der vorliegende Beitrag gibt einen kompakten Überblick über die wichtigsten Regelungsinhalte.

### Risikobasierter Ansatz

Der von der EU-Kommission vorgelegte Entwurf enthält Vorschriften für das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen der künstlichen Intelligenz (KI). Der Verordnung liegt ein risikobasierter Ansatz zu Grunde. Das bedeutet, dass nur dort regulatorische Belastungen festgelegt werden, wo Risiken für die Grundrechte von natürlichen Personen oder die Gefährdung von sensiblen Rechtsgütern erwartet werden. Vorgesehen sind insgesamt drei Risikoklassen (siehe Abbildung 1). KI-Praktiken, die als unannehmbar gelten, werden verboten. Für KI-Systeme mit einem hohen Risiko gelten Mindestanforderungen, welche durch Anbieter und Nutzer der Systeme umgesetzt werden müssen. Daneben gelten unabhängig von der Risikoklasse Transparenzvorgaben für bestimmte KI-Systeme (z. B. ChatBots). KI-Systeme mit einem geringen Risiko unterliegen keiner Regulierung.

### Auf was bezieht sich die Verordnung?

Die Verordnung regelt das Inverkehrbringen und den Einsatz von Systemen der künstlichen Intelligenz (sog. KI-Systeme). Die in der Verordnung verwendete Definition von KI-Systemen ist sehr weit gefasst und betrifft prinzipiell jede Software, die nach deterministischen Vorgaben funktioniert und Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann. Entscheidend für die Einordnung als KI-System ist, dass das System bestimmte Techniken und Konzepte verwendet. Diese werden im Anhang I der Verordnung aufgeführt. Hierzu zählen

- Konzepte des maschinellen Lernens,
- logik- und wissensgestützte Konzepte sowie
- statistische Ansätze.

Werden derartige Techniken und Konzepte eingesetzt, ist der sachliche Anwendungsbereich eröffnet und Anbieter und Nutzer von derartigen Systemen müssen die Vorgaben der Verordnung umsetzen.

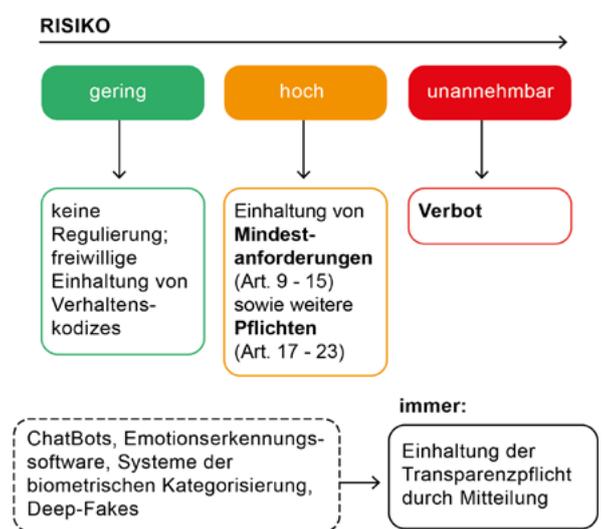


Abbildung 1: Risikoklassen und Folgen

1 <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=DE>

## **Für wen gilt die Verordnung?**

Durch die Verordnung werden vorrangig Anbieter von KI-Systemen in die Pflicht genommen, also solche Akteure, die ein KI-System entwickeln oder entwickeln lassen und das System in Verkehr bringen oder in Betrieb nehmen wollen. Daneben gilt die Verordnung auch für Nutzer von KI-Systemen, also solchen Akteuren, die ein KI-System in eigener Verantwortung verwenden. Nutzer können also beispielsweise Plattformen sein, die KI-Systeme eines Anbieters im Rahmen ihrer Dienstleistung oder ihres Produkts integrieren.

## **Gilt die Verordnung auch für FuE-Vorhaben?**

Zum Schutz der Wissenschaftsfreiheit wurde im Rahmen eines Kompromissvorschlags<sup>2</sup> eine Forschungsklausel aufgenommen. Danach gilt die Verordnung nicht für KI-Systeme, die speziell für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden. Rein interne Forschungs- und Entwicklungstätigkeiten sind damit von den Vorgaben der Verordnung freigestellt. Das Forschungsprivileg gilt im Umkehrschluss nicht, wenn eine Außenwirkung eintritt, also eine Verbreitung oder Inbetriebnahme eines KI-Systems (auch nur mittelbar) vorgesehen ist.

## **Welche KI-Praktiken sind verboten?**

Bestimmte KI-Praktiken sind grundsätzlich verboten. Hierzu zählen Techniken, die darauf ausgerichtet sind, Personen zu manipulieren oder deren Schutzbedürftigkeit auszunutzen. Untersagt sind zudem KI-Systeme, die durch Behörden zum Zweck des „Social Scoring“ eingesetzt werden sollen. Schließlich ist auch der Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen untersagt.

## **Was sind Hochrisiko-KI-Systeme?**

Kern der Verordnung sind Vorschriften für KI-Systeme, mit denen ein hohes Risiko assoziiert wird und deren unsachgemäße Verwendung schwerwiegende Folgen hätte. Als Hochrisiko-KI-Systeme gelten u.a. solche Systeme, die im Bereich der allgemeinen und beruflichen Bildung eingesetzt werden.<sup>3</sup> Eine Konkretisierung hierzu findet sich in Anhang III Nr. 3 der Verordnung (siehe Prüfungsschema Anlage 1). Demnach gelten KI-Systeme als hochriskant,

- die für Entscheidungen über den Zugang oder die Zuweisung von Personen zu Einrichtungen der allgemeinen und beruflichen Bildung verwendet werden sollen;
- die für die Bewertung von Lernenden in Einrichtungen der allgemeinen und beruflichen Bildung und für die Bewertung der Teilnehmer an üblicherweise für die Zulassung zu Bildungseinrichtungen erforderlichen Tests verwendet werden sollen.

Bei der Klassifizierung von Hochrisiko-KI-Systemen sollte berücksichtigt werden, dass nur solche Systeme von der Verordnung adressiert werden, die über den Verlauf der Bildung und des Berufslebens einer Person entscheiden und daher ihre Fähigkeit beeinträchtigen können, ihren Lebensunterhalt zu sichern. Damit soll verhindert werden, dass die unsachgemäße Verwendung von KI-Systemen das Recht auf allgemeine und berufliche Bildung sowie das Recht auf Nichtdiskriminierung verletzen und historische Diskriminierungsmuster fortschreiben.<sup>4</sup> Zu prüfen ist daher, ob KI-Systeme der folgenden Fallgruppen eingesetzt werden sollen.

### Zugang oder Zuweisung zu Bildungseinrichtungen

KI-Systeme gelten als hochriskant, wenn sie über den Zugang oder die Zuweisung zu Bildungseinrichtungen entscheiden. Darunter fallen KI-Systeme, die festlegen, ob eine Person zu einer Bildungseinrichtung zugelassen wird oder nicht und hierfür Verfahren, wie etwa KI-gestützte Aufnahmetests oder Interviews eingesetzt werden. Erfasst werden aber auch KI-Systeme, die Einfluss auf den Zuordnungsprozess nehmen und damit festlegen, zu welcher konkreten Institution eine Person zugewiesen wird (z. B. Zuweisung einer Person zu einer bestimmten Schule).

---

2 <https://data.consilium.europa.eu/doc/document/ST-14278-2021-INIT/en/pdf>

3 Daneben werden auch weitere KI-Systeme als hochriskant klassifiziert etwa, wenn sie in kritischen Infrastrukturen eingesetzt werden oder wenn sie als Produkt oder Produktbestandteil Sicherheitsfunktionen übernehmen (vgl. Art. 6 i.V.m. Anhang III).

4 Vgl. Erwägungsgrund 35.

## Bewertungssysteme

Darüber hinaus gelten KI-Systeme als hochriskant, wenn sie für die Bewertung von Lernenden in Einrichtungen der allgemeinen und beruflichen Bildung eingesetzt werden. Gemeint sind damit vor allem Bewertungsvorgänge im Rahmen von Prüfungen oder Tests, die einzeln oder insgesamt in eine Benotung münden. Sinn und Zweck der Regelung ist es hingegen nicht, KI-Systeme im Bildungsbereich vollumfänglich einer strengen Regulierung zu unterwerfen. Dienen KI-Anwendungen der Förderung des Lernprozesses, der Prüfungsvorbereitung oder der Verbesserung der Selbsteinschätzung der Lernenden, handelt es sich nicht um ein Hochrisiko-KI-System. Hierzu muss allerdings sichergestellt werden, dass die Ergebnisse dieser Prozesse nicht (und auch nicht indirekt) in die Bewertung von Lernenden einfließen. Vor diesem Hintergrund ist es auch denkbar, mittels anonymisierter Prüfungsprozesse eine personenspezifische Bewertung auszuschließen.

## Tests für die Zulassung zu Bildungseinrichtungen

Daneben gelten auch solche KI-Systeme als hochriskant, die für Bewertung von Teilnehmenden an Tests bestimmt sind, die üblicherweise für die Zulassung zu Einrichtungen der allgemeinen und beruflichen Bildung erforderlich sind. Anknüpfungspunkt sind hierbei also Prüfungen, deren Bestehen Voraussetzung für die Zulassung zu einer Bildungseinrichtung sind. Dies können beispielsweise KI-gestützte Prüfungen über die Sprachfähigkeit einer Person sein, wenn das Bestehen der Prüfung Voraussetzung für die Zulassung zu einem Studiengang ist (z.B. TOEFL-Test als Voraussetzung für die Zulassung zu einem Anglistik-Studium).

## **Welche Anforderungen gelten für Hochrisiko-KI-Systeme?**

Handelt es sich bei den eingesetzten Anwendungen um Hochrisiko-KI-Systeme, müssen eine Reihe von Mindestanforderungen umgesetzt werden. Hierzu gehört:

- Einrichtung und Unterhaltung eines Risikomanagementsystems (Art. 9)
- Einhaltung von Qualitätskriterien in Bezug auf Daten und Daten-Governance (Art. 10)
- Erstellung einer technischen Dokumentation (Art. 11)
- Fähigkeit der Anwendung zur Protokollierung von Vorgängen und Ereignissen (Art. 12)
- Umsetzung von Transparenzvorgaben sowie Bereitstellung von Informationen für Nutzer (Art. 13)
- Möglichkeit der Überwachung des KI-Systems durch eine Aufsichtsperson (Art. 14)
- Gewährleistung der Genauigkeit, Robustheit und Cybersicherheit (Art. 15).

## **Welche Pflichten bestehen für Anbieter und Nutzer von Hochrisiko-KI-Systemen?**

Anbieter von Hochrisiko-KI-Systemen müssen sicherstellen, dass die o.g. Anforderungen an Hochrisiko-KI-Systeme umgesetzt werden. Darüber hinaus unterliegen sie einem weitreichenden Katalog an horizontalen Pflichten<sup>5</sup>:

- Einrichtung eines Qualitätsmanagementsystems (Art. 17)
- Pflicht zur Erstellung der technischen Dokumentation (Art. 18)
- Pflicht zur Durchführung einer Konformitätsbewertung<sup>6</sup> (Art. 19)
- Pflicht zur Vorhaltung von automatisch erzeugten Protokollen (Art. 20)
- Überwachungs- und Informationspflichten (Art. 21 und Art. 22)
- Kooperationspflicht mit Aufsichtsbehörden (Art. 23)

Nutzer von hochriskanten KI-Systemen müssen sicherstellen, dass das KI-System bestimmungsgemäß und im Einklang mit den Vorgaben des Anbieters verwendet wird. Im Falle von Störungen oder Fehlfunktionen ist der Anbieter hierüber zu informieren.

## **Transparenzpflichten für bestimmte KI-Systeme**

Für KI-Systeme mit spezifischen Manipulationsrisiken werden – unabhängig davon, ob sie als hochriskant eingestuft werden – Transparenzpflichten angeordnet. Insbesondere muss Nutzenden mitgeteilt werden, dass

---

5 Die jeweiligen Vorgaben werden ausführlicher im angebenen Artikel ausgeführt und sind der Verordnung (<https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52021PC0206&from=DE>) zu entnehmen.

6 Geprüft werden muss, ob die Anforderungen an Hochrisiko-KI-Systeme erfüllt werden. Der Anbieter führt dabei die Konformitätsbewertung in Eigenverantwortung durch. Die Einbeziehung einer notifizierenden Stelle ist nur bei KI-Systemen zur biometrischen Identifikation und Kategorisierung notwendig.

sie es mit einem KI-System zu tun haben, es sei denn, dies ist aufgrund der Umstände und des Kontexts der Nutzung offensichtlich. Nutzende müssen also vor der Verwendung des Systems darüber informiert werden, dass sie mit einer Software (und nicht mit einem Menschen) interagieren (z. B. beim Einsatz von ChatBots). Eine Informationspflicht besteht darüber hinaus auch gegenüber Verwendern von Emotionserkennungssoftware oder Systemen der biometrischen Kategorisierung. Zudem müssen manipulierte oder verfälschte Bild-, Ton- oder Videoinhalte (Deep-Fakes) kenntlich gemacht werden.

### **KI-Systeme mit geringem Risiko**

Für KI-Systeme, deren Inverkehrbringen oder Inbetriebnahme mit einem geringen Risiko verbunden ist, enthält die Verordnung keine verbindlichen Vorgaben. Anbieter und Nutzer können sich jedoch freiwillig Verhaltenskodizes unterwerfen, welche nach Verabschiedung der Verordnung entwickelt werden sollen.

### **Fazit und Ausblick**

Die KI-Verordnung hat das Potential, die Entwicklung und den Einsatz von KI-Anwendungen im Bildungsbereich nachhaltig zu beeinflussen. Digitale Bildungsplattformen sollten prüfen, ob sie Anwendungen entwickeln oder einsetzen, die als KI-System zu klassifizieren sind und damit dem Anwendungsbereich der Verordnung unterliegen. Dabei ist zu beachten, dass die Definition von KI-Systemen sehr weit gefasst ist und bereits herkömmliche Software hierunter fallen kann. Sollte es sich bei den Anwendungen um Hochrisiko-KI-Systeme handeln, sind künftig hohe Compliance-Anforderungen zu erfüllen. Zu beachten ist jedoch, dass selbst für Hochrisiko-KI-Systeme eine Sonderregelung vorgesehen ist, nach der bereits in Verkehr gebrachte oder in Betrieb genommene KI-Systeme nicht von der Verordnung erfasst werden.<sup>7</sup> Die Ausnahmeregelung greift allerdings nur, wenn die Systeme nach Ablauf der Übergangsfrist nicht wesentlich in ihrer Konzeption oder Zweckbestimmung geändert wurden. Die Verordnung befindet sich derzeit noch im Abstimmungsprozess mit dem Europäischen Parlament. Im Zuge dessen kann es zu weiteren Änderungen am Verordnungstext kommen. Die Auswirkungen der Verordnung werden damit erst nach Inkrafttreten in ca. zwei bis drei Jahren spürbar sein. Um die Folgen des Regulierungsvorhabens besser abschätzen zu können, sollte der weitere Umsetzungsprozess nachverfolgt werden.

---

7 vgl. Art. 83 Abs. 2.

# Anlage 1: Prüfungsschema KI-Verordnung

