

Startseite > News > KI-VO: Diese Pflichten und Verbote gelten ab Februar 2025

# KI-VO: Diese Pflichten und Verbote gelten ab Februar 2025

30.01.2025



Bild von Gerd Altmann auf Pixabay

*+++ Please find the English version below. +++*

Ab dem 2. Februar 2025 gelten die ersten zentralen Bestimmungen der Verordnung über künstliche Intelligenz (KI-VO): das Verbot bestimmter KI-Praktiken und Verpflichtungen zur **Jobs** Kompetenz von Beschäftigten. Was bedeutet das für Unternehmen und Behörden?

## Verpflichtung zur KI-Kompetenz

Für jeden, der KI-Systeme anbietet oder betreibt, wird KI-Kompetenz ab dem 2. Februar 2025 zur Pflicht. Das heißt, Unternehmen und Behörden müssen sicherstellen, dass ihre Mitarbeitenden die eingesetzte Technologie verstehen. Die geforderte Kompetenz bezieht sich dabei direkt darauf, zu welchem spezifischen Zweck die künstliche Intelligenz eingesetzt wird.

Wenn ein Online-Händler personalisierte Kundenempfehlungen mit KI erstellt, erfordert das andere Kompetenzen als beim Einsatz eines KI-gestützten Bewerber:innenmanagements durch einen Konzern. Entscheidend ist die verantwortungsbewusste Bewertung von Eignung, Risiken und Auswirkungen jedes KI-Systems. Das Ziel ist, ein Bewusstsein für die Chancen und Risiken von KI in Unternehmen und Behörden zu schaffen und künstliche Intelligenz mit Bedacht einzusetzen.

## Verbotene KI-Praktiken

Eine wichtige Regelung betrifft KI-Praktiken, die in der EU nun verboten sind. Diese konkreten Verbote gelten für jedes KI-System. Im Fokus stehen vor allem bestimmte **staatliche Überwachungspraktiken**; aber auch manipulative Beeinflussungen von Betroffenen und besonders schutzbedürftigen Personen wie Kindern und Jugendlichen, zum Beispiel im **Kontext sozialer Medien**.

## Staatliche Überwachungspraktiken

Die Verbote formen einen umfassenden Rahmen zum Schutz vor missbräuchlicher staatlicher KI-Nutzung, der über das klassische Datenschutzrecht hinausgeht. Besonders weitreichend ist das **Social Scoring-Verbot**: Behörden dürfen keine KI-Systeme nutzen, die etwa das Verhalten in sozialen Medien oder die Zahlungsmoral auswerten, um daraus Konsequenzen für Verwaltungsentscheidungen abzuleiten.

In Behörden und Schulen sind KI-Systeme verboten, die Emotionen der Mitarbeitenden oder Schüler:innen analysieren – etwa zur Leistungskontrolle oder Verhaltenssteuerung, wobei Ausnahmen für medizinische oder sicherheitsrelevante Gründe vorgesehen sind.

Die Polizei darf keine KI einsetzen, die allein aufgrund von Persönlichkeitsmerkmalen oder Verhaltensmustern vorhersagt, ob jemand Straftaten begehen könnte (sogenanntes *Predictive Policing*). Auch untersagt ist es, massenhaft Gesichtsbilder aus dem Internet oder von Überwachungskameras zu sammeln, um damit Erkennungsdatenbanken zu erstellen.

Die KI-VO verbietet zudem den KI-Einsatz, um Menschen mithilfe ihrer biometrischen Daten nach ihrer politischen Einstellung oder sexuellen Orientierung zu kategorisieren; enge Ausnahmen gelten für die Strafverfolgung.

Ähnlich ist es bei der KI-gestützten Echtzeit-Fernbiometrie in öffentlichen Räumen. Der Einsatz von Gesichtserkennung zum Beispiel bei Demonstrationen ist grundsätzlich verboten. **Jobs** Ausnahmen für Strafverfolgung und Gefahrenabwehr bedürfen einer zusätzlichen gesetzlichen Grundlage. Die KI-VO sieht vor, dass ein solches Gesetz zwingend Genehmigungsvorbehalte enthalten muss und die Datenschutzbehörden vor dem Einsatz solcher Systeme einbezogen werden müssen.

## KI-Verbote und soziale Medien

Auch für Unternehmen zeigt die KI-VO rote Linien auf: Für sie gilt das Verbot der Emotionsanalyse bei Mitarbeitenden. Außerdem sind manipulative KI-Praktiken, die menschliche Schwächen ausnutzen, nun verboten. Besonders der Schutz vulnerabler Gruppen wie Kinder und Jugendliche vor KI-gesteuerten Beeinflussungsversuchen steht im Fokus. Diese Verbote zielen darauf ab, die Autonomie und Integrität von Betroffenen zu schützen.

Eine KI-gestützte Content-Empfehlung in sozialen Medien kann verboten sein, wenn sie die typischen Schwächen von Minderjährigen wie Unerfahrenheit oder fehlende Impulskontrolle ausnutzt, um deren Nutzungsverhalten zu intensivieren – vorausgesetzt, diese längere Verweildauer führt zu erheblichen Schäden; etwa durch die vermehrte Anzeige von Inhalten, die zu gesundheitsschädlichem oder riskantem Verhalten animieren. Die KI-VO geht dabei weiter als das Datenschutzrecht oder der Digital Services Act und untersagt solche Praktiken präventiv und absolut.

## Durchsetzung und Konsequenzen

Diese Verbote für Staat und Wirtschaft markieren eine klare Grenze: KI soll das Leben erleichtern und Prozesse optimieren, aber nicht zur Manipulation oder zur Ausnutzung von Schwächen eingesetzt werden. Verstöße können nicht nur zu Sanktionen nach der KI-VO führen, sondern auch die Datenschutzbehörden auf den Plan rufen. Auf verbotene Praktiken gerichtete Datenverarbeitungen sind mangels legitimen Zwecks niemals datenschutzkonform.

Für die KI-Kompetenz gilt [Art. 4 KI-VO](#) , die Verbote sind in [Art. 5 KI-VO](#)  geregelt.

+++

## AI Act: Obligations and Prohibitions Taking Effect in February 2025

Starting February 2, 2025, the first key provisions of the Artificial Intelligence Act (AI Act) will take effect: the prohibition of certain AI practices and obligations regarding AI literacy of employees. What does this mean for companies and public authorities?

### AI Literacy Requirements

From February 2, 2025, AI literacy becomes mandatory for anyone who provides or deploys AI systems. This means companies and public authorities must ensure their staff understand the technology they are using. The required competency directly relates to the specific purpose for which the AI system is being deployed. For instance, when an online retailer uses AI for personalized customer recommendations, it requires a different level of literacy than a corporation using AI-powered recruitment management systems. The key is responsible assessment of the suitability, risks, and impacts of each AI system. The goal is to create

awareness of AI opportunities and risks within organizations and to ensure AI systems are used with care.

## Prohibited AI Practices

Certain AI practices are now prohibited in the EU. These specific prohibitions apply to every AI system. They primarily focus on certain government surveillance practices, but also cover manipulative influences on affected individuals and particularly vulnerable persons such as children and adolescents, for example in the context of social media.

### Government Surveillance Practices

The prohibitions create a comprehensive framework for protection against misuse of AI by government authorities, going beyond traditional data protection law. Particularly far-reaching is the ban on social scoring: Authorities may not use AI systems that evaluate behavior on social media or payment history to derive detrimental consequences for administrative decisions.

In government agencies and schools, AI systems that analyze emotions of employees or students are prohibited - for instance for performance monitoring or behavior control; though exceptions are provided for medical or safety-related reasons.

Law enforcement may not use AI to predict potential criminal activity solely based on personality traits or behavioral patterns (known as *Predictive Policing*). It is also prohibited to scrape facial images from the internet or surveillance cameras to create recognition databases.

The AI Act also prohibits the use of AI systems to categorize people based on their political views or sexual orientation using their biometric data; exceptions apply for law enforcement purposes.

Similarly, AI-powered real-time remote biometric identification in public spaces is regulated. The use of facial recognition, for example for demonstrations in public spaces, is prohibited in principle. Exceptions for law enforcement and emergency responses require an additional legal basis. The AI Act stipulates that such legislation must include mandatory approval requirements and data protection authorities must be consulted before deploying such systems.


### AI Prohibitions and Social Media

The AI Act also draws red lines for the private sector: The ban on emotion analysis of employees applies to companies as well. Additionally, manipulative AI practices that exploit human vulnerabilities are now prohibited. Particular focus is placed on protecting vulnerable groups such as children and adolescents from AI-driven manipulation attempts. These prohibitions aim to protect the autonomy and integrity of affected individuals.

AI-powered content recommendations on social media can be prohibited if they exploit typical vulnerabilities of minors, such as inexperience or lack of impulse control, to intensify their usage behavior – provided this increased engagement leads to significant harm; for example, through increased exposure to content that encourages harmful or risky behavior. The AI Act goes beyond data protection law or the Digital Services Act by preventively and absolutely prohibiting such practices.

## Enforcement and Consequences

These prohibitions for both government and business establish a clear boundary: AI should enhance our lives and improve processes, it must not be used for manipulation or exploitation. Violations can not only lead to sanctions under the AI Act but also trigger action from data protection authorities. Data processing that is directed at these prohibited practices cannot be compliant with data protection laws as it lacks a legitimate purpose.

The AI competency requirements are now governed by [Article 4 AI Act](#) , while the prohibitions are set out in [Article 5 AI Act](#). 