

Europäische KI-Verordnung und ihre Operationalisierung

Workshopreihe: Europäische KI-Verordnung und ihre Operationalisierung

Mit Verabschiedung der KI-Verordnung im Dezember kommen neue regulatorische Herausforderungen auf Unternehmen zu, die KI einsetzen. Während es nach Inkrafttreten Übergangsfristen zur Umsetzung der neuen Vorgaben geben wird, ist eine gute Vorbereitung wichtig, um die vielfältigen Chancen durch den Einsatz von KI-Modellen adäquat abzusichern und die Nutzung vertrauenswürdig zu gestalten.

In dieser Workshopreihe wollen wir gemeinsam mit Wissenschaft, Industrie und Anwender*innen Möglichkeiten zur technischen Umsetzung der KI-Verordnung erarbeiten und dabei auch darauf eingehen, wie man Compliance schon während der Anwendungsentwicklung adressieren kann.

Die Workshopreihe soll dabei drei verschiedene Thematiken beleuchten, die für die Umsetzung der KI-Verordnung essenziell sind. Im ersten Workshop werden Urheberrechtsverletzungen durch Generative KI mit Blick auf aktuelle Modelle thematisiert, weiter geht es mit der technischen Prüfung von rechtlichen Fairnessanforderungen im zweiten Workshop und die Reihe abschließen wird ein Workshop zur Entwicklung und Prüfung von Anwendungen mit generativer KI. Die Workshopreihe richtet sich neben den Partnern und assoziierten Partnern des ZERTIFIZIERTE KI-Projektes an alle interessierten Expert*innen.

1. Workshop: Generative KI und Urheberrecht

Foundation-Modelle erobern die KI-Welt im Sturm und finden in kürzester Zeit immer neue Weiterentwicklungen und Anwendungsmöglichkeiten. Gleichzeitig werden auch Probleme und Schwachstellen offenbar, die mit diesem Paradigmenwechsel einhergehen. Die Tendenz der riesigen Modelle, sich die Trainingsdaten zu merken und sie entsprechend reproduzieren zu können, kann beispielsweise zu Urheberrechtsverletzungen führen, wenn die Trainingsdaten auch urheberrechtlich geschütztes Material enthalten.

Dieser Workshop soll mit Blick auf die KI-Verordnung mögliche Urheberrechtsprobleme mit generativer KI zunächst aufzeigen und anschließend technisch beleuchten, was der aktuelle Stand der State-of-the-Art Modelle bezüglich Verwendung und Reproduktion von urheberrechtlich geschütztem Material ist.

Termin: 10. April 2024

2. Workshop: Technische Prüfung von Fairnessanforderungen

KI-Modelle übernehmen in Personalauswahl, Medizin und vielen weiteren Feldern zunehmend mehr Aufgaben, bei denen diskriminierende Entscheidungen der KI nicht nur moralisch fragwürdig sind, sondern auch rechtliche Konsequenzen nach sich ziehen können. Mögliche Ungleichbehandlungen in Modellausgaben, die aus Verzerrungen in den Trainingsdaten oder Fehlern in den Modellen entstehen, machen Fairnessbetrachtungen somit zu einer maßgeblichen Säule der Vertrauenswürdigkeit aktueller und kommender Modelle. In diesem Workshop soll aufgezeigt werden, wie sich die Fairnessanforderungen aus geltendem Recht und kommender KI-Verordnung technisch umsetzen lassen.

Termin: 19. Juni 2024

3. Workshop: Entwicklung und Prüfung von Anwendungen mit generativer KI

Der Aufstieg generativer Modelle bringt eine Vielzahl neuer regulatorischer und sicherheitstechnischer Herausforderungen mit sich, die bei Nutzung in eigenen Anwendungen wiederum neue Ansätze zur Prüfung und Methoden zur Anwendungsentwicklung erfordern. Auch von der KI-Verordnung werden diese Modelle als sogenannte „General Purpose AI“ gesondert behandelt.

Um Compliance mit der KI-Verordnung- zu gewährleisten, ist wichtig, Vertrauenswürdigkeit und Absicherung bereits früh im Entwicklungsprozess im Blick zu haben.

Dieser Workshop gibt dabei einen Überblick zu Herausforderungen, Prüfansätzen und Vertrauenswürdigkeitsaspekten für Anwendungen, die generative KI nutzen.

Termin: 11. September 2024

Gefördert durch:

Ministerium für Wirtschaft,
Industrie, Klimaschutz und Energie
des Landes Nordrhein-Westfalen

