BSI

Leitfaden zur Datenqualität in KI-Systemen

[04.07.2025] Das Bundesamt für Sicherheit in der Informationstechnik stellt erstmals eine systematische Hilfestellung bereit, um Qualitätsanforderungen aus der EU-KI-Verordnung (AI Act) in der Entwicklung von KI-Systemen technisch umzusetzen und dokumentierbar zu machen.

Eine Schlüsselrolle für die Leistungsfähigkeit von künstlicher Intelligenz spielen die verwendeten Trainingsdaten – riesige, speziell aufbereitete Datensätze, die in das jeweilige KI-Modell eingespeist werden und diesem dann zum „Lernen“ zur Verfügung stehen. Die europäische KI-Verordnung – auch bekannt als AI Act – von 2024 definiert Qualitätsanforderungen an KI-Trainingsdaten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nun einen eigenen Katalog zur Qualitätssicherung von Trainingsdaten in KI-Anwendungen veröffentlicht. Die Dokumentenreihe mit dem Titel „Qualitycriteria for AI Trainingsdata in AI Lifecycle“ (kurz: QUAIDAL) bietet eine systematische Überführung der im AI-Act formulierten abstrakten Qualitätsanforderungen in konkrete Bausteine, Maßnahmen und Metriken und Methoden. So soll die gezielte Einhaltung regulatorischer Vorgaben unterstützt und deren technische Nachvollziehbarkeit im Entwicklungsprozess von KI-Systemen erhöht werden. „Wir müssen sicherstellen, dass Anwendungen mit Künstlicher Intelligenz hohen Qualitätsanforderungen entsprechen. Nur so können wir vertrauenswürdige KI herstellen und nutzen. Das BSI bietet mit diesem Katalog eine ganz konkrete Hilfestellung, die an der Basis ansetzt“, so die BSI-Präsidentin Claudia Plattner.

Besonders für Hochrisiko-Systeme

QUAIDAL richtet sich insbesondere an Anbieter von Hochrisiko-KI-Systemen, für welche die KI-Verordnung detaillierte Anforderungen hinsichtlich Dokumentation, Datenmanagement und kontinuierlicher Qualitätssicherung definiert. Durch die modulare Gestaltung des Leitfadens können Projektverantwortliche und Entwicklungsteams frühzeitig passende Maßnahmen zur Sicherstellung der Datenqualität auswählen und deren Umsetzung systematisch nachweisen. Darüber hinaus lässt sich dieses modulare Konzept zukünftig flexibel erweitern, um neue technologische Entwicklungen zu berücksichtigen. Als nationale Cyber-Sicherheitsbehörde unterstützt das BSI mit QUAIDAL öffentliche Stellen und Unternehmen dabei, regulatorische Anforderungen umzusetzen und vertrauenswürdige KI-Anwendungen zu entwickeln. Das BSI lädt die Community explizit zur aktiven Mitwirkung ein – es können Vorschläge für eigene Bausteine, Maßnahmen und Metriken eingebracht werden.

(sib)

Stichwörter: Künstliche Intelligenz, AI-Act, BSI