KI-Qualität sichern, aber wie?

Dr. Cord Schlötelburg

Frankfurt am Main, 03.09.2025

AIQ | AI QUALITY & TESTING HUB

Was ist KI-Qualität?

KI-Qualität beschreibt den Grad, in dem ein KI-System zuverlässig, vertrauenswürdig, leistungsfähig und im Einklang mit ethischen sowie regulatorischen Standards arbeitet.

Funktionale Qualität

Genauigkeit & Präzision: Korrektheit der KI-Ergebnisse im Vergleich zu einer bekannten Wahrheit oder zu einem definierten Ziel?	**Beispiel:** KI zur Erkennung von Hautkrebs
Robustheit: Reaktion des Systems auf Störungen, ungewöhnliche Eingaben oder Rauschen in den Daten?	**Beispiel:** KI zur Verkehrszeichenerkennung bei selbstfahrenden Autos
Generalisierungsfähigkeit: Ergebnisqualität der KI auch bei neuen, zuvor unbekannten Daten	**Beispiel:** KI zur Erkennung von Überschwemmungsflächen aus Satellitenbildern

Technische Qualität

Performance: Antwortzeiten, Rechenaufwand, Skalierbarkeit	**Beispiel:** KI-gestützte Routenplanung in einer Navigations-App
Wartbarkeit: Wie leicht lässt sich das Modell aktualisieren, verbessern oder debuggen?	**Beispiel:** KI-gestützte Erkennung von Gebäudeschäden nach Naturkatastrophen
Nachvollziehbarkeit: Dokumentation von Architektur, Trainingsdaten, Hyperparametern und Änderungen.	**Beispiel:** KI zur Paket-Routenoptimierung bei einem Lieferdienst

Vertrauens- und Sicherheitsaspekte

Erklärbarkeit: Kann nachvollzogen werden, warum die KI eine bestimmte Entscheidung trifft?	**Beispiel:** KI-gestützte Kreditvergabe bei einer Bank
Fairness und Bias-Kontrolle: Werden diskriminierende Verzerrungen erkannt und minimiert?	**Beispiel:** KI-gestützte Bewerberauswahl in einem Unternehmen
Datenschutz und Sicherheit: Einhaltung von DSGVO, Schutz sensibler Daten, Absicherung gegen Angriffe.	**Beispiel:** Sprach-KI im Kundenservice einer Versicherung

Ethische und gesellschaftliche Qualität

Transparenz: Offenlegung der Grenzen und Risiken der KI.	**Beispiel:** KI gestützte Social Media Moderation.
Verantwortlichkeit: Klare Zuständigkeiten bei Fehlern oder Schäden.	**Beispiel:** Unfall mit autonomen Fahrzeugen
Nachhaltigkeit: Energieeffizienz und Ressourcenschonung beim Training und Betrieb.	**Beispiel:** Training von großen Sprachmodellen

Warum ist KI Qualität für Anbieter wichtig?

- **Wettbewerbsvorteil & Kundenbindung**:
  zuverlässige KI steigert Kundenzufriedenheit und fördert langfristige Verträge.
- **Reduzierung von Haftungs- & Reputationsrisiken:**
  minimiert finanzielle Schäden und Imageverluste.
- **Erfüllung gesetzlicher & regulatorischer Anforderungen:**
  vermeidet Strafen und Nachrüstkosten.
- **Skalierbarkeit & Wartbarkeit:**
  schnellere Anpassung an neue Märkte und Anwendungen.
- **Vertrauensaufbau & Markenimage:**
  starke Marktposition durch nachweislich faire und sichere KI.

Wie kann man vorgehen, um KI Qualität zu sichern?

- Anforderungsanalyse
- Datenqualitätsmanagement
- Modellentwicklung
- Test
- Monitoring im Betrieb
- Dokumentation

Anforderungsanalyse

Bevor man mit der KI-Entwicklung startet, muss klar sein:

- Was soll die KI können? (z. B. Bilder klassifizieren, Texte zusammenfassen, Betrug erkennen)
- Welche Qualitätsziele gibt es? (z. B. Genauigkeit, Reaktionszeit, Fairness-Anforderungen)
- Welche Risiken müssen vermieden werden? (z. B. Diskriminierung, Fehlalarme, Sicherheitslücken)
- Regulatorische Vorgaben (z. B. EU-KI-Verordnung, DSGVO)

💡 Ziel: Alle Beteiligten haben ein gemeinsames Verständnis von Zweck, Erfolgskriterien und Grenzen der KI.

Datenqualitätsmanagement

Die Qualität der Daten ist entscheidend für die Qualität der KI.

- Datenquellen prüfen: Sind sie aktuell, vollständig, repräsentativ?
- Fehler und Ausreißer entfernen: z. B. falsche Werte, doppelte Einträge.
- Label-Qualität sichern: korrekte Beschriftung der Trainingsdaten sicherstellen.
- Bias-Kontrolle: Prüfen, ob bestimmte Gruppen über- oder unterrepräsentiert sind.
- Dokumentation der Datenherkunft (Data Lineage).

💡 Ziel: Das Modell lernt aus sauberen, aussagekräftigen und ausgewogenen Daten.

Modellentwicklung

Während der Entwicklung werden Qualitätsprüfungen eingebaut:

- Trainings- und Testdaten trennen, um Überanpassung (Overfitting) zu vermeiden.
- Metriken definieren, die den späteren Einsatzzweck widerspiegeln.
- Robustheitstests: z. B. mit gestörten oder leicht veränderten Eingaben prüfen.
- Fairness-Analysen durchführen
- Explainability-Methoden einbauen, um Entscheidungen nachvollziehbar zu machen.

💡 Ziel: Das Modell ist nicht nur leistungsfähig, sondern auch robust, fair und erklärbar.

Test und Validierung

Bevor das Modell live geht, muss es gründlich geprüft werden:

- Technische Tests: Funktionieren Schnittstellen und Datenflüsse fehlerfrei?
- Leistungstests: Erreicht das Modell die definierten Qualitätskennzahlen?
- Szenario-Tests: Simulation realer Einsatzbedingungen, inklusive Extremfällen.
- Unabhängige Validierung: Tests durch ein anderes Team als die Entwickler.

💡 Ziel: Sicherstellen, dass die KI unter realistischen Bedingungen wie gewünscht funktioniert.

Monitoring im Betrieb

Die Qualitätssicherung endet nicht mit dem Go-Live:

- Leistung überwachen: Kennzahlen wie Genauigkeit oder Reaktionszeit regelmäßig messen
- Daten-Drift erkennen: Prüfen, ob sich Eingabedaten im Laufe der Zeit stark verändern
- Fehler- und Vorfallmanagement: Auffällige Entscheidungen oder Sicherheitsvorfälle untersuchen
- Feedback-Loops: Nutzerfeedback nutzen, um das Modell zu verbessern

💡 Ziel: Frühzeitig Verschlechterungen erkennen und gegensteuern.

Dokumentation

Eine lückenlose Dokumentation ist wesentlich für Nachvollziehbarkeit und Compliance:

- Anforderungen und Qualitätsziele
- Datenbeschreibung: Herkunft, Auswahl, Vorverarbeitung
- Modellbeschreibung: Architektur, Trainingsparameter, Versionen
- Testergebnisse: inkl. Metriken, Testplänen, Besonderheiten
- Betriebsprotokolle: Monitoring-Ergebnisse, Änderungen, Zwischenfälle

💡 Ziel: Transparenz für interne Teams, Auditoren und ggf. Behörden

→ gesetzliche Rahmenbedingungen für KI-Systeme

Quality-by-Design ←→ Compliance-by-Design

Es gibt in der EU keine „Zulassung“ von KI-Systemen, sondern:

- Die EU stellt gesetzliche Anforderungen an KI-Systeme
- Der Hersteller / Anbieter erklärt selbst, dass sein Produkt diese Anforderungen erfüllt
- Eine Benannte Stelle bestätigt (ggf.), ob das auch zutrifft
- Der Hersteller / Anbieter bringt die CE-Kennzeichnung an und vermarktet das KI-System

Die EU KI-Verordnung

Was müssen Anbieter von Hoch-Risiko KI-Systemen beachten? (1)

- Risikomanagementsystem, Art. 9
- Daten und Daten-Governance, Art. 10
- Technische Dokumentation, Art. 11
- Aufzeichnungspflichten, Art. 12
- Transparenz und Bereitstellung von Informationen für die Betreiber, Art. 13
- Menschliche Aufsicht (Mensch-Maschine-Schnittstelle), Art. 14
- Genauigkeit, Robustheit und Cybersicherheit, Art. 15
- Kennzeichnungsvorschriften, ---
- Qualitätsmanagementsystem, Art. 17
- Dokumentenführung, ---
- Automatisch erzeugte Protokolle, Art. 19

Die EU KI-Verordnung

Was müssen Anbieter von Hoch-Risiko KI-Systemen beachten? (2)

- Konformitätsbewertung, Art. 43
- EU-Konformitätserklärung, Art. 47
- CE-Kennzeichnung, Art. 48
- Registrierung, Art. 49 (1)
- Korrekturmaßnahmen und Informationspflicht sowie Zusammenarbeit mit den zuständigen Behörden, Art. 20
- Konformitätsnachweis gegenüber der zuständigen nationalen Behörde, ---
- Pflichten der Betreiber, Art. 26
- Marktüberwachung und Kontrolle von KI-Systemen auf dem Unionsmarkt (Marktüberwachungsbehörden), Art. 74
- Überwachung nach dem Inverkehrbringen und Vigilanz (Anbieter), Art. 72, 73

Wie bringt man ein KI-System konform auf den EU Markt?

Roadmap

Wie gehe ich vor?

Zweck

Was genau soll die KI tun?

Qualifizierung

Handelt es sich um ein KI-System?

Risiken

Welche Risikokategorie gilt?

Gesetze

Welche Gesetze, Richtlinien und Normen gelten?

Akteure

Wer trägt welche Verantwortung?

Pflichten

Welche Anforderungen müssen im Detail erfüllt werden?

Konformität

Wie komme ich zur CE Kennzeichnung?

Überwachung

Was passiert nach dem Inverkehrbringen?

Markt

Welche besonderen Aspekte sind beim Marktzugang ggf. zu berücksichtigen?

Bringen Sie Ihr KI-System auf den europäischen Markt. Mit Qualität und Compliance.

AIQ – Künstliche Intelligenz und Qualität

Unsere Schwerpunkte:

- Testen von KI-Systemen
- Entwicklung von KI-Testverfahren
- Entwicklung von RAG-Systemen
- Unterstützung bei KI-Compliance-Anforderungen

Kontakt: info@aiqualityhub.com

Vielen Dank für ihre Aufmerksamkeit

Ihr Ansprechpartner:
Dr. Cord Schlötelburg
Geschäftsführer
AI Quality & Testing Hub GmbH

Bessie-Coleman-Strasse 7
60549 Frankfurt am Main
info@aiqualityhub.com
www.aiqualityhub.com