Bundesverband
Gesundheits-IT – bvitg e. V.

bvitg-Stellungnahme

Community-Draft A5 (AI Audit and Assurance Assesment Architecture)

Kontakt
Kora Reinicke
Referentin eHealth
kora.reinicke@bvitg.de

bvitg.de

Der Bundesverband Gesundheits-IT – bvitg e. V. nimmt zum Community-Draft A5 wie folgt Stellung:

Community-Draft A5 (AI Audit and Assurance Assessment Architecture)

Über die A5-Prüfarchitektur

Der neue A5 des BSI soll eine standardisierte, modulare Prüfarchitektur schaffen, mit der die Vertrauenswürdigkeit von KI-Systemen systematisch, nachvollziehbar und im Einklang mit regulatorischen Anforderungen – wie dem EU AI Act – bewertet und nachgewiesen werden kann. Er umfasst drei Dokumente:

- Horizontales Trustworthiness Basismodul: In diesem Dokument werden die Anforderungen an vertrauenswürdige KI ausformuliert.
- Betriebsmodul Cloud-Infrastruktur: In diesem Dokument werden die zusätzlichen Anforderungen an KI, die in der Cloud betrieben wird, ausformuliert.
- Prüfmethodik: In diesem Dokument wird die anzuwendende Prüfmethodik beschrieben.

Zurzeit liegen die Dokumente als Community Draft vor.

Einordnung

Der bvitg begrüßt die Initiative des BSI, die Vertrauenswürdigkeit von KI-Anwendungen in einer strukturierten, standardisierten und überprüfbaren Form zu überprüfen. Grundsätzlich unterstützt der bvitg die Standardisierung sowie einen transparenten und sicheren Einsatz von Technologien, wie der Künstlicher Intelligenz. In der derzeit vorliegenden Ausgestaltung des A5 sieht der bvitg jedoch an verschiedenen Stellen Anpassungs- und Weiterentwicklungsbedarf, den wir mit den nachfolgenden Anmerkungen adressieren möchten.

Kritikpunkte

Der aktuelle Entwurf des A5 stellt sich als zusätzlicher Prüfkatalog, neben bereits bestehenden Prüflandschaften, dar. Überschneidungen mit bestehenden Evidenzen finden keine Berücksichtigung, mögliche Harmonisierungen werden nicht konsequent zusammengeführt. Doppelprüfungen werden insbesondere für die Cloud als gleiches Kriterium neben C5 angeführt:

- **Parallelregulierung, insbesondere für die Cloud:** Der A5 droht, eine zusätzliche Prüflandschaft neben bestehenden regulatorischen und normativen Anforderungen (z.B. EU MDR, C5) zu schaffen und damit Doppelprüfungen, Bürokratie und Kosten zu erhöhen.

- **Unzureichende Harmonisierung und Evidenznutzung:** Überschneidungen mit bestehenden Zertifizierungen und Testierungen (z.B. EU MDR, C5) und bestehenden Normen (insbesondere auch mit den gerade in Entwicklung befindlichen harmonisierten Normen für den AI Act) etc. werden nicht konsequent zusammengeführt; bereits vorhandene Prüfungen, Zertifizierungen und Evidenzen werden nicht ausreichend anerkannt und wiederverwendet.

- **Doppelprüfungen insbesondere für die Cloud:** Im Betriebsmodul Cloud wird das C5-Testat als Kriterium angeführt. Im C5 werden Risikomanagement, Qualitätsmanagement etc. ausreichend adressiert. Lediglich der Punkt der "Human Oversight" sollte hier noch abgeprüft werden müssen.

Verbesserungsvorschläge

- **A5 als integrierenden „Assurance Layer" etablieren:** Bestehende Zertifizierungen, Testierungen und Normen sollten in einer gemeinsamen Architektur zusammengeführt werden, statt ähnliche Kriterien in einer vollständig, neuen Prüflandschaft aufzubauen.

- **Prüfung konsequent auf das Delta begrenzen:** Für jedes A5-Control sollte ausgewiesen werden, was durch bestehende Anforderungen und Evidenzen vollständig, teilweise oder nicht abgedeckt ist. Nur das verbleibende Delta sollte zusätzlich geprüft werden müssen.

- **Prinzip der Evidenzwiederverwendung verankern:** Qualitativ geeignete Nachweise sollten unabhängig von ihrem ursprünglichen Prüfkontext mehrfach verwendet werden können („audit once, use often").

- **Think European:** Der AI Act ist eine europäische Verordnung, viele Aktivitäten zur Stärkung von KI werden auf europäischer Ebene vorgenommen. Ein Kriterienkatalog zur Bewertung der Vertrauenswürdigkeit von KI sollte unbedingt auch auf europäischer Ebene vereinheitlicht werden, um zersplitterte Anforderungen der Einzelstaaten zu vermeiden.

Zusammenfassung

Vertrauenswürdigkeit von KI-Anwendungen ist für die Gesundheits-IT ein zentrales, aber mehrdimensionales Thema: Es geht nicht allein um Standards und Transparenz, sondern gleichermaßen um regulatorische Kohärenz und Innovationsfähigkeit auf europäischer Ebene. Der bvitg befürwortet einen risikobasierten, horizontalen Ansatz, der bestehende Nachweise nutzt, die Anbieter nicht überproportional belastet und den Zugang zu innovativen Technologien nicht erschwert. Ziel muss es sein einen Rahmen zu schaffen, der Vertrauen, Sicherheit und Versorgungsfähigkeit stärkt, ohne die Innovations- und Wettbewerbsfähigkeit der europäischen Gesundheits-IT zu gefährden.