

HRAIS-Leitlinien: Probleme aus Sicht des ZVEI/VDMA

Die vorliegenden Hochrisiko-KI-Leitlinien der EU-Kommission (HRAIS-Leitlinien) schaffen nach Einschätzung von VDMA/ZVEI keine belastbare Orientierung. Stattdessen erweitern sie den Anwendungsbereich von Art. 6(1) AI Act durch eine Reihe von weitreichenden Auslegungen. Diese sind aus unserer Sicht weder vom Gesetzestext gedeckt noch berücksichtigen sie die Ergebnisse des Omnibus-Prozesses ausreichend. Die Leitlinien sollten keine neue Regulierungsebene schaffen, sondern präzise erklären, wann Art. 6(1) AI Act tatsächlich ausgelöst wird.

Der Entwurf berücksichtigt insbesondere weder die neue Whitelisting-Regel in Art. 6(1a) AI Act noch die Verschiebung der Verordnung (EU) 2023/1230 (Machinery Regulation) von Annex I Teil A nach Annex I Teil B. Auch ist das vorgegebene Feedback-Format unzureichend, da das Online-Formular pro Absatz maximal 500 Zeichen und pro Kapitel höchstens fünf kommentierbare Absätze zulässt. Am Beispiel von Kapitel III.2.2 (19 Absätze) wird deutlich, dass rund drei Viertel des Textes praktisch nicht kommentiert werden können. Darüber hinaus fehlt die Möglichkeit, eigene Positionspapiere hochzuladen.

Im Folgenden werden drei besonders gravierende Probleme dieser Leitlinien diskutiert:

1. (33): Abweichende Definition von Sicherheitsbauteil

Die Leitlinien behaupten in (33), der AI Act enthalte eine autonome Definition des Begriffs „Sicherheitsbauteil“ und gehe insoweit den Definitionen in anderen Gesetzen vor (*lex specialis*). Genau hier liegt aus Sicht von VDMA/ZVEI ein erhebliches Problem, das über die Hochrisiko-KI-Leitlinien hinausgeht und die Grundstruktur des New Legislative Frameworks (NLF) verändert: Das NLF arbeitet seit Jahrzehnten mit sektorspezifischen, technisch operationalisierten Definitionen, etwa im Maschinen- und Aufzugsrecht. Würde (33) gelten, müssten innerhalb eines Produkts zwei Safety-Component-Definitionen parallel angewandt werden: eine für die KI-Komponente, eine für den übrigen Produktteil. Der KI-Omnibus hat den Vorrang der sektoralen Gesetzgebung im Bereich der Maschinenverordnung zudem deutlich bestätigt. Auch die in Art. 8 der Machinery Regulation vorgesehene Anknüpfung an „this regulation“ spricht dafür, die Definitionen des jeweiligen sektoralen Rechtsakts heranzuziehen; zudem untermauert Erwägungsgrund 64 des AI Acts eine komplementäre, nicht verdrängende Rolle des Verordnungstextes.

2. (56-59): Unzulässige Ausdehnung von Art. 6(1)

In den Paragraphen 56-59 führen die Leitlinien die Begriffe „*appropriate/enhanced regulatory scrutiny*“ und „*equivalent mechanism*“ ein. Diese Begriffe sind im AI Act nicht definiert und verschieben die Regulierungsschwelle des Art. 6(1)(b).

- Art. 6(1)(b) verlangt, dass das Produkt einer Konformitätsbewertung durch Dritte („Third-Party Conformity Assessment“) unterliegen muss. Das Modul A (interne Fertigungskontrolle) löst diese Voraussetzung gerade nicht aus. Die (56) und (57) dürfen daher nicht so gestaltet werden, als könne eine interne Kontrolle durch harmonisierte Normen einer Drittprüfung gleichgestellt werden.
- (58) wiederholt die Idee einer „*enhanced scrutiny*“ durch Drittprüfung oder „*equivalent mechanisms*“. Das widerspricht aus VDMA/ZVEI-Sicht der Logik des NLF und Decision 768/2008/EC, wonach Konformitätsbewertungsmodule risikoproportional gewählt werden.
- (59) stützt sich auf eine Formulierung der Richtlinie 2025/2509 (Toy Safety Regulation), die die interne Fertigungskontrolle bei Anwendung harmonisierter Normen als Opt-out von Drittprüfung erscheinen lässt. Der NLF und entsprechend der Blue Guide behandeln die Module jedoch als Varianten, nicht als Abweichung von einem Drittprüfungs-Default. Die unglückliche Formulierung der Toy Safety Regulation sollte auf keinen Fall in den revidierten NLF einfließen.

3. HRAIS-Kapitel 3.2, Abs. 187 und zu Abs. 38: unvollständige Auswertung von Erwägungsgrund 55

Die Leitlinien zitieren Erwägungsgrund 55 mehrfach, lassen aber nach der Stellungnahme an entscheidender Stelle die Einschränkung außer Acht, dass bestimmte Komponenten „not necessary in order for the system to function“ sind. In Paragraph 187 der HRAI Leitlinien und in der Fußnote zu Paragraph 38 wird zwar der Ausschluss reiner Cybersecurity-Komponenten erwähnt; die funktionale Notwendigkeit wird jedoch nicht systematisch ausgewertet.