DIN EN ISO/IEC 23894:2025-07 (D)

Informationstechnik - Künstliche Intelligenz - Leitlinien für Risikomanagement (ISO/IEC 23894:2023); Deutsche Fassung EN ISO/IEC 23894:2024

Inhalt

Seite

Europäisches Vorwort 7

Vorwort 8

Einleitung 9

1 Anwendungsbereich 10

2 Normative Verweisungen 10

3 Begriffe 10

4 Grundsätze des KI-Risikomanagements 10

5 Rahmenwerk 14
5.1 Allgemeines 14
5.2 Führung und Verpflichtung 14
5.3 Integration 15
5.4 Gestaltung 15
5.4.1 Verstehen der Organisation und ihres Kontextes 15
5.4.2 Artikulieren der Risikomanagementverpflichtung 18
5.4.3 Zuweisung von organisatorischen Rollen, Befugnissen, Verantwortlichkeiten und Rechenschaftspflichten 18
5.4.4 Zuordnung von Ressourcen 18
5.4.5 Einrichten der Kommunikation und Konsultation 19
5.5 Implementierung 19
5.6 Bewertung 19
5.7 Verbesserung 19
5.7.1 Anpassen 19
5.7.2 Fortlaufendes Verbessern 19

6 Risikomanagementprozess 19
6.1 Allgemeines 19
6.2 Kommunikation und Konsultation 19
6.3 Anwendungsbereich, Kontext und Kriterien 20
6.3.1 Allgemeines 20
6.3.2 Festlegen des Anwendungsbereichs 20
6.3.3 Externer und interner Kontext 20
6.3.4 Festlegen von Risikokriterien 21
6.4 Risikobeurteilung 22
6.4.1 Allgemeines 22
6.4.2 Risikoidentifikation 22
6.4.3 Risikoanalyse 25
6.4.4 Risikobewertung 27
6.5 Risikobehandlung 27
6.5.1 Allgemeines 27
6.5.2 Auswahl von Maßnahmen zur Risikobehandlung 27
6.5.3 Erstellen und Implementieren von Plänen zur Risikobehandlung 27
6.6 Überwachen und Überprüfen 27
6.7 Aufzeichnen und Berichten 27

Anhang A (informativ) Ziele 29

A.1 Allgemeines ... 29
A.2 Verantwortlichkeit ... 29
A.3 KI-Expertise ... 29
A.4 Verfügbarkeit und Qualität von Trainings- und Testdaten ... 29
A.5 Auswirkung auf die Umwelt ... 30
A.6 Fairness ... 30
A.7 Instandhaltungsfreundlichkeit ... 30
A.8 Datenschutz ... 30
A.9 Robustheit ... 31
A.10 Sicherheit (Safety) ... 31
A.11 Sicherheit (Security) ... 31
A.12 Transparenz und Erklärbarkeit ... 31

Anhang B (informativ) Risikoquellen ... 33
B.1 Allgemeines ... 33
B.2 Komplexität der Umgebung ... 33
B.3 Fehlende Transparenz und Erklärbarkeit ... 33
B.4 Automatisierungsgrad ... 34
B.5 Risikoquellen in Bezug auf maschinelles Lernen ... 34
B.6 System-Hardwareprobleme ... 35
B.7 System-Lebenszyklusprobleme ... 35
B.8 Technologische Reife ... 36

Anhang C (informativ) Risikomanagement und Lebenszyklus von KI-Systemen ... 37

Literaturhinweise ... 40

Tabellen

Tabelle 1 — Anwendung von Risikomanagementgrundsätzen auf künstliche Intelligenz ... 11

Tabelle 2 — Zu prüfende Punkte bei der Festlegung des externen Organisationskontextes ... 15

Tabelle 3 — Zu prüfende Punkte bei der Festlegung des internen Kontextes einer Organisation ... 16

Tabelle 4 — Zusätzliche Leitlinien zum Festlegen von Risikokriterien ... 21

Tabelle C.1 — Risikomanagement und Lebenszyklus von KI-Systemen ... 37