

Inhaltsverzeichnis

Vorwort	5
Überblick	9
Modul A Kontext	17
A.1 Zielgruppen: Für wen ist dieses Playbook?	17
A.2 Einleitung	18
A.3 Warum KI heute in fast jeder IT-Beschaffung steckt	20
A.4 Immer nüchtern bleiben	23
A.4.1 Komplexe Verwaltungs- bzw. Bestandssysteme	24
A.4.2 Urteilsvermögen: Warum KI perfekte Sätze schreibt, aber die Welt nicht versteht ..	25
A.4.3 ChatGPT, Claude, Grok & Co. vs. Intelligenztests	26
Modul B Grundlagen – KI für Nicht-ITler	29
B.1 Begriffsdefinitionen	29
B.2 Inkompetenz zweiten Grades	31
B.3 KI vs. IT mit KI-Anteilen	34
B.4 Neue Funktion oder alte Funktion?	35
B.5 Arten von KI: Regelbasiert, Lernend, Generativ & Co.	37
B.6 Training von KI-Systemen: Datenqualität ist der Schlüssel	38
B.7 Blackbox und Explainable AI: Ist KI transparent?	41
B.7.1 Transparenz von KI in Beschaffungsverfahren	42
B.7.2 Rechtliche und inhaltliche Verantwortung sowie Kontrolle	42
B.8 Kontextfenster: Definition und Beschaffungsfolgen	42
B.9 Antrainierte vs. entstehende Fähigkeiten von KI	45
B.10 Halluzinationen – oder etwa nicht?	47
B.10.1 Konfabulationen	47
B.10.2 Warum wissen KIs nicht alles?	47
B.10.3 Statistische Vorhersage vs. zielorientierte Verzerrung	48
B.10.4 Wege um Konfabulation zu vermeiden	49
B.11 IT-Sicherheit und KI	51
B.11.1 Realbeispiele	51
B.11.1.1 Datendiebstahl (Exfiltration) durch Mitarbeiter: Samsung & ChatGPT	51
B.11.1.2 Indirekte Prompt Injection und serverseitige Exfiltration	52
B.11.1.3 Reputationsschaden durch Jailbreaking: DPD Chatbot	52
B.11.2 Angriffsseite	52
B.11.2.1 Daten- und Modellintegrität	54
B.11.2.2 Agenten- und Tool-Missbrauch: Autonomie als Waffe	54
	13

B.11.2.3 Die multimodale Dimension: Neue Angriffsflächen	55
B.11.3 Verteidigungsseite	55
B.11.3.1 Neudefinition der Vertrauensgrenzen: Zero Trust für KI-Outputs	56
B.11.3.2 Härtung der Wissensbasis: Sicherheit für Retrieval Augmented Generation (RAG)	56
B.11.3.3 Just-in-time Access oder Transaktionelle Berechtigungen	57
B.11.3.4 Zwischenfazit	58
B.11.3.5 AI Red Teaming	59
B.11.3.6 Forensik und Governance: AIBOM und Observability	60
B.11.4 Konkrete Implikationen für KI-Beschaffung	60
Modul C Chancen und Risiken von KI	61
C.1 Chancen / Vorteile	62
C.2 Risiken / Herausforderungen	62
C.3 Exkurs: Wie kann KI in der Beschaffung helfen?	64
C.3.1 Ein Blick auf die Phasen einer Vergabe	64
C.3.2 Technische Realität und Marktlage	65
C.3.3 Kernanwendungsfall für die Praxis	67
C.3.4 Chancen für Vergabestellen	67
C.3.5 Risiken und offene Fragen	67
C.3.6 Fazit	68
C.4 Cloud vs. On-Premises	68
C.4.1 IT-Sicherheit im Kontext Cloud vs. On-Premises	69
C.4.2 Weiterentwicklung und Release-Management	70
C.4.3 Betrieb und Personal	71
C.4.4 Investitions- und Betriebskosten	72
C.4.5 Hybridlösungen: RAG-Architektur, Varianten	75
C.4.6 Recht & Compliance	77
C.4.7 Fazit	79
C.5 KI-Reifegrad: Wie bereit sind Organisation und Technik?	81
C.5.1 Organisatorischer KI-Reifegrad	81
C.5.2 Technischer Reifegrad der KI-Lösung	83
C.6 Rechtliche Grundlagen	85
C.6.1 Datenschutz (DSGVO) – Umgang mit personenbezogenen Daten	85
C.6.2 EU AI Act – stufenweise Regulierung der KI	86
C.6.3 Haftung und Verantwortlichkeit	88
C.7 Vergabegrundsätze – fairer Wettbewerb trotz KI	89
Modul D Beschaffungsphasen und Leistungsphasen	91
D.1 Phase: Planung der Beschaffung	91
D.1.1 Bedarfsdefinition: Was ist Ihr Anwendungsfall?	93

D.1.2	Analyse des Ist-Zustands und der Rahmenbedingungen	94
D.1.3	Risikoanalyse: Was kann kritisch werden?	96
D.1.4	Markterkundung: Den KI-Markt verstehen, bevor man ausschreibt	98
D.1.5	Die Grenzen einer Markterkundung	98
D.1.6	Strategische Weichenstellungen	100
D.2	Phase: Design der Beschaffung	103
D.2.1	Leistungsbild und Losbildung: Was wird genau ausgeschrieben?	103
D.2.2	Vorwort zu Formulierungen und Kriterien	105
D.2.3	Leistungsbeschreibung: KI-Anforderungen formulieren	106
D.2.4	Eignungs- und Zuschlagskriterien	109
D.2.4.1	Eignungskriterien: Welche Voraussetzungen müssen KI-Anbieter erfüllen?	109
D.2.4.2	Zuschlagskriterien: Wie bewerten wir KI-Mehrwert und Leistung?	111
D.2.5	Bewertungsmethode und Bewertungsansatz auswählen	113
D.2.5.1	Punktevergaben	115
D.2.5.2	Leistungsbewertungsmatrix erstellen	116
D.2.6	Hilfsweise Bewertung	116
D.2.7	Vertragsmodelle und EVB-IT	117
D.2.7.1	Überblick: Grundsätzliche Vertragsarten und EVB-IT im KI-Kontext	118
D.2.7.2	Allgemeines	119
D.2.7.3	KI-spezifische Vertragsklauseln zu Haftung, IP-Rechten, Exit-Strategie ...	122
D.2.7.4	Retraining und Updates: Wie bleibt die KI aktuell?	125
D.2.7.5	Service Level Agreements (SLAs) für KI-Leistungen	126
D.2.7.6	Letzte Punkte zu vertraglichen Aspekten	127
D.3	Phase: Durchführung eines Vergabeverfahrens	128
D.3.1	Angebotsphase: Bieterfragen und Angebotsprüfung	128
D.3.2	Angebotsbewertung: Die richtige Lösung herausfiltern	130
D.3.2.1	Qualitative Aspekte in KI-Evaluation	131
D.3.2.2	Bewertung ohne Verhandlung (z.B. offenes Verfahren)	131
D.3.2.3	Bewertung im Verhandlungsverfahren	132
D.3.3	Zuschlag und Verfahrensabschluss	133
D.4	Phase: Projektierung	134
D.4.1	Vom Zuschlag bis zum Projektstart	135
D.4.2	Die Rolle hybrider Ansätze	136
D.4.3	KI-Schwerpunkt oder nachgeordneter KI-Anteil	137
D.4.4	Zusammenarbeit und Kommunikation	137
D.4.5	Vorbereitung des Übergangs	138
D.4.6	Pilotphasen und schrittweiser Übergang	138
D.4.7	Betriebsübergang und Change Management	139
D.4.8	Fazit	140

- D.5 Phase: Betrieb, Monitoring & Governance** 141
 - D.5.1 Monitoring: Überwachung der KI im laufenden Betrieb 141
 - D.5.2 Governance: Leitlinien, Verantwortlichkeiten, Ethik 143
- D.6 Fazit: Empfehlungen / Best Practice** 145
- D.7 Checklisten** 147
 - D.7.1 KI-Checkliste Entscheidungshilfe On-Premises vs. Cloud vs. Hybrid für RAG-Systeme 147
 - D.7.2 KI-Checkliste: Bedarfsermittlung 149
 - D.7.3 KI-Fragenliste zu KI-übergreifenden Sicherheitsaspekten 152
 - D.7.4 KI-Checkliste Sicherheitsaspekte für (hybride) RAG-Systeme 154
 - D.7.5 KI-Checkliste: Beschaffungskonzeption 157
 - D.7.6 KI-Checkliste: Eignungskriterien 159
 - D.7.7 KI-Checkliste: Zuschlagskriterien 161
 - D.7.8 KI-Checkliste: Vertragsgestaltung 163
 - D.7.9 KI-Checkliste: Zuschlag und Abschluss des Vergabeverfahrens 166
- Modul E Glossar & FAQ** 169
 - E.1 Glossar** 169
 - E.2 FAQ (Häufige Fragen)** 176