

Praxishandbuch

KI-VO

Künstliche Intelligenz rechtskonform im privaten
und öffentlichen Bereich einsetzen

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhalt

Vorwort	XV
1 Was ist KI und wie unterscheiden sich Datenwissenschaft und Datenanalytik?	1
<i>Gabriele Bolek-Fügl</i>	
1.1 Die Bausteine der KI	2
1.1.1 Daten	3
1.1.2 Algorithmen	5
1.1.3 Rechenleistung	7
1.1.4 Speicher	7
1.1.5 Messung und Modelloptimierung	8
1.1.6 Schnittstellen zur Interaktion	8
1.1.7 Sicherheit und Datenschutz	9
1.2 Datenwissenschaft und Datenanalytik	10
1.3 Entwicklung von KI in KMUs	11
2 Geopolitik der künstlichen Intelligenz	17
<i>Veronica Cretu</i>	
2.1 Entstehende Landschaft von KI-Vorschriften	18
2.2 Das Rennen um die KI-Regulierung – die großen Drei	22

3	KI-Verordnung: Rechte und Pflichten	33
	<i>Gabriele Bolek-Fügl, Veronica Cretu, Julia Fuith, Merve Taner, Natascha Windholz, Carina Zehetmaier</i>	
3.1	Einführung zur KI-VO	34
3.1.1	Definition von KI-Systemen	39
3.1.2	Rollen von natürlichen oder juristischen Personen	40
3.1.3	Phasen der Markteinführung	42
3.1.4	Begriffe zur Nutzung von KI-Systemen	43
3.1.5	Datenbezogene Bezeichnungen	45
3.1.6	KI-Kompetenz	47
3.2	KI-Kompetenz für Anbieter	48
3.2.1	Einführung	49
3.2.2	Definition von KI-Kompetenz	52
3.2.3	KI-Kompetenz und die Bestimmungen der KI-VO	54
3.2.4	Vorschlag für ein Reifegrad-Framework für KI-Anbieter	56
3.3	Risikobasierter Ansatz	62
3.3.1	Verbotene KI-Systeme	62
3.3.2	Hochrisiko-KI-Systeme	69
3.3.2.1	Einstufung von KI als Hochrisiko-KI-System	69
3.3.2.2	Anhang III	73
3.3.2.3	Anforderungen an Hochrisiko-KI-Systeme	80
3.4	Grundrechtliche Folgenabschätzung	95
3.4.1	KI-VO und Grundrechte	96
3.4.1.1	Durchführung der Grundrechte-Folgenabschätzung ...	98
3.4.1.2	Folgenabschätzung als Teil von KI-Governance	108
3.4.1.3	Bereits bestehende Tools für Grundrechts- Folgenabschätzung	108
3.5	Harmonisierte Normen, Konformitätsbewertung, Bescheinigungen und Registrierung	110
3.5.1	Harmonisierte Normen und CE-Kennzeichnung	112
3.5.2	Konformitätsbewertungsverfahren	115
3.5.3	Ausnahmen vom Konformitätsbewertungsverfahren	118
3.5.4	EU-Konformitätserklärung	119
3.5.5	Registrierung	121

3.6	Transparenzverpflichtungen in der KI-VO	122
3.6.1	Leitlinien für die Umsetzung der Transparenzpflichten zu Daten und Datenverwaltung	125
3.6.2	Leitlinien für die Umsetzung der in Art. 13 KI-VO vorgesehenen Transparenzbestimmungen	127
3.6.3	Leitlinien zur Umsetzung der Transparenzpflichten für Anbieter und Bereitsteller bestimmter KI-Systeme und GPAI-Modelle	130
3.7	General Purpose Artificial Intelligence (GPAI)	132
3.7.1	ChatGPT: Beginn einer „KI-Revolution“? – Auswirkungen auf den Gesetzgebungsprozess	132
3.7.2	Aufnahme von GPAI in die KI-VO	134
3.7.3	KI-Modelle und KI-Systeme für den allgemeinen Verwendungszweck	135
3.7.3.1	Einstufungsvorschriften für GPAI-Modelle	135
3.7.3.2	Verpflichtungen	137
3.7.4	GPAI-Modelle mit systemischem Risiko	141
3.7.4.1	Einstufungsvorschriften für KI-Modelle mit allgemeinem Verwendungszweck mit systemischem Risiko gemäß Art. 51 KI-VO	141
3.7.4.2	Verpflichtungen für GPAI-Modelle mit systemischem Risiko gemäß Artikel 55	143
3.7.5	GPAI-Modelle und Hochrisiko-Systeme	144
3.7.6	Umsetzungsfrist und Strafen	144
3.8	KI-Reallabore	145
3.8.1	Einrichtung und Funktionsweise	146
3.8.2	Weiterverarbeitung von personenbezogenen Daten	149
3.8.3	Tests außerhalb von KI-Reallaboren	150
3.8.4	Einwilligungen zu Tests außerhalb von Reallaboren	152
3.8.5	Erleichterungen für KMUs	152
3.9	Behörden	153
3.9.1	Notifizierende Behörde	153
3.9.2	Konformitätsbewertungsstellen und notifizierte Stellen	154
3.10	Governance in der KI-VO	158
3.10.1	KI-Büro	158
3.10.2	KI-Gremium	158
3.10.2.1	Zusammensetzung	158
3.10.2.2	Aufgaben des KI-Gremium	159

3.10.3	Beratungsforum	160
3.10.4	Wissenschaftliches Gremium	161
3.10.5	Nationale Behörden	161
3.10.6	EU-Datenbank für Hochrisiko-KI-Systeme	162
3.10.7	Beobachtung nach Inverkehrbringen des KI-Systems	162
3.10.8	Austausch von Informationen über schwerwiegende Vorfälle ...	163
3.10.9	Rechtsdurchsetzung	164
3.10.10	Vertraulichkeit von Verfahren	165
3.10.11	Verfahren auf nationaler Ebene für den Umgang mit KI-Systemen, die ein Risiko bergen	166
3.10.12	Verfahren für KI-Systeme, die vom Anbieter nicht als Hochrisiko-KI klassifiziert wurden	167
3.10.13	Konforme KI-Systeme, die ein Risiko bergen	167
3.10.14	Formale Nichtkonformität	168
3.10.15	Rechtsmittel	168
	3.10.15.1 Recht auf Erklärung einer Entscheidung	168
	3.10.15.2 Rechtsmittel bei GPAI	169
3.11	Strafen und Sanktionen	170
3.12	KMUs und Start-ups in der KI-VO	173
	3.12.1 Erleichterungen und Ausnahmen für KMUs und Start-ups	174
	3.12.2 Checkliste: neues KI-System nach der KI-VO auf den Markt bringen	176
4	Datenschutz	183
	<i>Gabriele Bolek-Fügl</i>	
4.1	Allgemeine Anforderungen der DSGVO	185
	4.1.1 Grundsätze für die Verarbeitung personenbezogener Daten ...	187
	4.1.2 Rechtmäßigkeit der Verarbeitung	192
	4.1.3 Informationspflicht bei Erhebung personenbezogener Daten ...	194
	4.1.4 Rechte der betroffenen Personen	195
4.2	Datenschutz durch Technikgestaltung	197
	4.2.1 Privacy by Design und Privacy by Default	197
	4.2.2 Verantwortung für die gesetzeskonforme Verarbeitung	199
4.3	Anforderungen für Testdaten	201
4.4	Automatisierte Entscheidungsfindung	202

4.5	Orientierungshilfen und Empfehlungen der Datenschutz- Aufsichtsbehörden zu DSGVO und KI	206
4.5.1	Veröffentlichungen des European Data Protection Boards (Auszug)	206
4.5.2	Empfehlungen der DSK	209
4.5.3	Der Landesbeauftragte für Datenschutz und Informations- freiheit Baden-Württemberg	213
4.5.4	Hamburgischer Beauftragter für Datenschutz zu LLMs	213
4.5.5	FAQ der österreichischen Datenschutzbehörde	216
4.6	ChatGPT und die Datenschutzbeschwerde von noyb	217
5	Geistiges Eigentum	221
	<i>Alexandra Ciarnau</i>	
5.1	Schutz der KI und ihrer Komponenten	222
5.1.1	Urheber- und Leistungsschutzrechte	224
5.1.1.1	Allgemeines	224
5.1.1.2	Individuell entwickelte KI-Systeme	224
5.1.1.3	Individuell entwickelte KI-Modelle	224
5.1.1.4	Input- und Trainingsdatenpool	225
5.1.1.5	Anwenderdokumentation und Benutzerhandbuch	225
5.1.1.6	Rechte und Ansprüche des Urhebers bzw. der Urheberin	226
5.1.1.7	Rechteeinräumung	227
5.1.1.8	Open-Source-Software	228
5.1.1.9	Patent- und Gebrauchsmusterschutz	228
5.1.2	Geschäftsgeheimnisschutz	229
5.2	Legal IP-Compliance beim Einsatz von KI	230
5.2.1	KI-Input-Seite	231
5.2.1.1	IP-rechtlich geschützte Input-Daten	231
5.2.1.2	KI-VO-Anforderungen an KI-Systeme	233
5.2.2	KI-Output-Seite	233
5.3	Checkliste	236
5.4	Referenztablelle Rechtsvorschriften	237

6	KI und IT-Vertragsrecht	241
	<i>Alexandra Ciarnau, Merve Taner</i>	
6.1	Lizenzierung von Standardsoftware	243
6.2	Softwareentwicklung	246
6.3	Softwarewartung	248
6.4	Open-Source-Software	249
6.4.1	Open-Source-KI – Wegbereiter für die Zukunft?	250
6.4.2	Definition von Open Source und Rechtsgrundlage	252
6.4.3	Rechtliche Problemfelder im Zusammenhang mit Open Source nach bereits existierenden Rechtsgrundlagen	253
6.4.4	Open-Source-Software-Strategie der Europäischen Kommission	257
6.4.5	Ausnahmen für Open Source in der KI-VO	257
6.5	Hardwarekauf und -wartung	260
6.6	Allgemeines zur Haftung	261
6.7	Referenztablette Rechtsvorschriften	264
7	Privater Sektor	267
	<i>Kristina Altrichter, Gabriele Bolek-Fügl, Karin Bruckmüller, Alexandra Ciarnau, Julia Eisner, Isabella Hinterleitner, Manuela Machner, Renate Rechinger, Carina Zehetmaier, Kludia Zotzmann-Koch</i>	
7.1	KI – von Vorurteilen zur Diskriminierung	267
7.1.1	Recht auf Gleichheit und Nichtdiskriminierung	273
7.1.2	Wie Vorurteile ihren Weg in die KI finden	276
7.1.2.1	Wie die KI-Verordnung Diskriminierung adressiert ...	279
7.1.2.2	Can we fix bias in AI?	282
7.2	Einsatz von KI in der Finanzbranche	285
7.2.1	Ausnahmen vom Anwendungsbereich	286
7.2.2	Verbotene KI-Systeme	288
7.2.3	Hochrisiko-KI-Systeme	291
7.2.3.1	Klassifizierung	291
7.2.3.2	Widerlegung der Hochrisiko-Eigenschaft	294
7.2.3.3	Wechselwirkungen zwischen Finanzregularien und der KI-VO	295
7.2.4	KI-Systeme/-Modelle mit allgemeinem Verwendungszweck	296
7.2.5	Bestimmte KI-Systeme	297
7.2.6	Behördenkompetenzen	297

7.3	KI im Versicherungswesen	298
7.3.1	Dynamic Underwriting und Risikoprüfung in der Krankenversicherung	300
7.4	KI und Whistleblowing	303
7.4.1	Whistleblower für die Kategorie KI	307
7.4.2	Einsatzgebiete von KI bei der Umsetzung der EU-Whistleblowing-Richtlinie	310
7.4.2.1	Herausforderungen im Whistleblowing-Prozess	310
7.4.2.2	Ablauf des Whistleblowing Use Case	313
7.5	Einsatz von KI bei zukünftigen und bestehenden Arbeitsverhältnissen ..	316
7.5.1	Verfassen von Stellenanzeigen mit KI	318
7.5.2	KI-Unterstützung bei Bewerberauswahl mittels Videoanalyse ...	320
7.6	Einsatz von KI in der Bildung	323
7.6.1	Rollen in der KI-VO	325
7.6.2	KI-Kompetenz (Art. 4 KI-VO)	326
7.6.3	KI-Systeme mit „begrenztem“ Risiko in der Bildung	327
7.6.4	Hochrisiko-KI-Systeme in der Bildung	328
7.6.5	Verbotene KI-Systeme in der Bildung	332
7.7	KI im Gesundheitswesen	333
7.7.1	Beispiel: KI-Diagnose von Hauterkrankungen	334
7.7.1.1	Hochrisiko-KI-Einstufung im Sinne der KI-VO	335
7.7.1.2	Anforderungen und Pflichten des Krankenhaus- betreibers nach der KI-VO	335
7.8	KI in der Werbung	339
7.8.1	Rechtliche Vorgaben für KI in der Werbung	340
7.8.1.1	Verbotene KI-Systeme	340
7.8.1.2	Schnittmengen mit weiteren Gesetzen	341
7.8.1.3	Datenhandel	342
7.8.1.4	Personalisierung	343
7.8.2	Energieverbrauch und Nachhaltigkeit	343
7.8.3	Best Practice: Generative KI in der Kreation	344
7.9	Tourismus	346
7.9.1	Use Case: Operative Effizienz	347
7.9.2	Use Case: Gästeerlebnisse	354
7.9.3	Use Case: Smarte Betriebe	358

7.10	Einsatz von KI beim autonomen Fahren	362
7.10.1	Österreichische & internationale Gesetzgebung	364
7.10.2	Entwicklung autonomer Fahrfunktionen	365
7.10.3	Die KI-VO und autonomes Fahren	367
8	Öffentlicher Sektor	369
	<i>Kristina Altrichter, Karin Bruckmüller, Veronica Cretu, Theresa Tisch, Natascha Windholz</i>	
8.1	„Public Decision-Making“ und KI	369
8.1.1	Anwendungsfälle in Anhang III der KI-VO	370
8.1.2	Beispiel: Vergabe von Sozialleistungen	371
8.1.3	Beispiel: Vergabe von Kindergartenplätzen („Kitaplätze“)	373
8.2	Einsatz von KI in der Strafverfolgung	374
8.2.1	Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme	375
8.2.2	Umsetzungspflichten der Mitgliedstaaten	378
8.3	Einsatz von KI bei Wahlen und demokratischen Prozessen	378
8.3.1	Aufkommende Diskussionen über die Auswirkungen von KI auf Demokratie und Wahlprozesse	379
8.3.2	Wie ist KI im Zusammenhang mit Wahlen zu definieren?	382
8.3.3	Nutzung der Chancen und Minimierung von Risiken durch KI-Einsatz	382
8.3.4	KI und Integrität von Wahlen: eine hypothetische Analyse des Cambridge Analytica-Skandals im Rahmen der KI-VO	389
8.4	Einsatz von KI im NIS-Sektor	394
8.4.1	Einführung NIS und NIS 2	394
8.4.1.1	NIS2	395
8.4.2	Bedeutung von NIS2 für die Lieferkette	397
8.4.3	Einsatz von KI in NIS-Unternehmen	398
8.4.3.1	Anhang I KI-VO	398
8.4.3.2	Anhang III KI-VO	399
9	Ethik	403
	<i>Gabriele Bolek-Fügl, Valerie Hafez, Sabine Singer</i>	
9.1	Ethik-Leitlinien für vertrauenswürdige KI	403
9.1.1	Worum geht es?	404
9.1.2	Ethische Grundsätze der Leitlinien	405
9.1.3	Kernanforderungen	406

9.1.4	Methoden zur Umsetzung der Kernanforderungen	409
9.1.5	Werkzeuge für die Umsetzung	410
9.2	Relevante KI-Richtlinien & Policys	413
9.2.1	Empfehlung des OECD-Rats zu künstlicher Intelligenz	413
9.2.2	The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence	416
9.2.3	Compliance-Werkzeuge für viele Gelegenheiten	419
9.2.4	Artificial Intelligence Risk Management Framework	424
9.2.5	Weitere prägende Ethik-Richtlinien	426
9.3	EU- und weltweite Organe, Gremien und Ausschüsse	429
9.4	Vom Digitalen Humanismus zum wertebasierten KI-System	431
9.4.1	Value-based Engineering	433
9.4.2	Vorteile und strategische Bedeutung von Value-based Engineering	436
9.4.3	Fazit	438
10	Governance im Unternehmen	439
	<i>Gabriele Bolek-Fügl, Karin Bruckmüller, Veronica Cretu, Valerie Hafez, Klaudia Zotzmann-Koch</i>	
10.1	Praxisbeispiel: Beurteilung eines Use Cases nach der KI-VO	439
10.1.1	Beschreibung des Use Cases: KI-gestützte Brandfrüherkennung und Alarmierungssystem	440
10.1.2	Wie geht man an die Bearbeitung heran?	440
10.1.3	Fazit	450
10.2	Risikomanagement, menschliche Aufsicht und nützliche Werkzeuge	451
10.2.1	Governance im Lebenszyklus eines KI-Systems einbetten	452
10.2.2	Risiken erkennen und adressieren	453
10.2.2.1	Annäherungen an Risiken, Vorfälle, Unfälle und Betroffenheiten	453
10.2.2.2	Risiken messen	455
10.2.2.3	Verantwortung bei Vorfällen und Unfällen	456
10.2.2.4	Unbekanntes wahrnehmen und kontrollieren	457
10.2.3	Menschliche Aufsicht	458
10.2.3.1	Aufsicht aufschlüsseln	460
10.2.3.2	Aufsichtskompetenzen entwickeln und beibehalten ...	461
10.2.3.3	Aufsicht kontextsensibel gestalten	462

10.2.3.4	Externe bei der Aufsicht einbinden	462
10.2.3.5	Menschliche Aufsicht: Für und Wider	464
10.2.4	Fazit	465
10.3	Daten- und Wissensmanagement	467
10.3.1	Säulen des Data Governance Frameworks	473
10.4	Audit von künstlicher Intelligenz	479
10.4.1	Grundsätzliches zum Audit	480
10.4.2	Audit-Team	481
10.4.3	Unterschied Risikomanagement und Audit	482
10.4.4	Hilfreiche Audit-Checklisten	483
10.4.5	Praktisches Beispiel einer einfachen KI-Audit-Checkliste	485
10.5	Verhaltenskodex/Code of Conduct	489
10.5.1	Beispiel eines Code of Conduct für den Einsatz von künstlicher Intelligenz im Unternehmen	493
10.5.2	Weitere Betrachtungen zum KI-Verhaltenskodex	498
10.6	KI und Nachhaltigkeit	499
10.6.1	ESG – Environmental, Social and Corporate Governance	500
10.6.2	Diversität, Inklusion, Gerechtigkeit	501
10.6.3	Nutzen für die Umwelt	502
10.6.4	Hochrisiko-KI-Systeme	503
10.6.5	Lieferketten	504
10.6.6	Fazit	505
11	Die Autorinnen	507
	Index	513