

<b>Vorwort</b> .....	<b>11</b>
----------------------	-----------

---

## **Teil I Was ist MLOps, und warum wird es benötigt?**

<b>1 Warum jetzt, und was sind die Herausforderungen?</b> .....	<b>15</b>
MLOps – Definition und Herausforderungen .....	16
MLOps zum Reduzieren von Risiken .....	20
Risikobeurteilung .....	20
Risikominderung .....	21
Responsible AI durch MLOps .....	22
MLOps zur Skalierung von Machine-Learning-Modellen .....	23
Abschließende Überlegungen .....	24
<b>2 An MLOps-Prozessen beteiligte Personen</b> .....	<b>25</b>
Fachexperten .....	27
Data Scientists .....	29
Data Engineers .....	31
Software Engineers .....	32
DevOps .....	33
Modellrisikomanager/Auditor .....	34
Machine Learning Architects .....	34
Abschließende Überlegungen .....	35
<b>3 Die Kernkomponenten von MLOps</b> .....	<b>37</b>
Eine Einführung in Machine Learning .....	37
Modellentwicklung .....	38
Festlegen von Geschäftszielen .....	38
Datenquellen und explorative Datenanalyse .....	38
Feature Engineering und Feature Selection .....	40
Training und Evaluierung .....	40
Reproduzierbarkeit .....	40
Responsible AI .....	41

Überführung in die Produktion und Deployment .....	42
Arten und Elemente des Modell-Deployments .....	42
Anforderungen beim Deployment von Modellen .....	44
Monitoring .....	44
Verantwortungsbereiche des DevOps-Teams .....	45
Verantwortungsbereiche des Data-Science-Teams .....	45
Verantwortungsbereiche der Managementebene .....	47
Iteration und Lebenszyklus .....	47
Iteration .....	48
Die Feedback-Schleife .....	49
Governance .....	50
Daten-Governance .....	52
Prozess-Governance .....	53
Abschließende Überlegungen .....	54

---

## Teil II MLOps einsetzen

<b>4 Modellentwicklung .....</b>	<b>57</b>
Was genau sind Machine-Learning-Modelle? .....	58
Theoretischer Hintergrund .....	58
Einsatz in der Praxis .....	59
Erforderliche Komponenten .....	60
Unterschiedliche ML-Algorithmen – unterschiedliche MLOps-Herausforderungen .....	61
Explorative Datenanalyse .....	63
Feature Engineering und Feature Selection .....	64
Feature-Engineering-Techniken .....	64
Wie die Auswahl der Features die MLOps-Strategie beeinflusst ...	65
Experimente .....	67
Modelle evaluieren und vergleichen .....	68
Ein geeignetes Qualitätsmaß auswählen .....	69
Gegenprüfen des Modellverhaltens (Cross-Checking) .....	71
Auswirkungen von Responsible AI auf die Modellentwicklung ...	72
Versionsverwaltung und Reproduzierbarkeit .....	75
Abschließende Überlegungen .....	77
<b>5 Vorbereitung für die Produktion .....</b>	<b>79</b>
Laufzeitumgebungen .....	80
Modelle aus der Entwicklungs- in die Produktivumgebung überführen .....	80

Datenzugriff vor Validierung und Inbetriebnahme in der Produktion . . . . .	82
Abschließende Überlegungen zu Laufzeitumgebungen . . . . .	83
Risikobeurteilung von Modellen . . . . .	83
Der Zweck der Modellvalidierung . . . . .	83
Die Risikotreiber bei Machine-Learning-Modellen . . . . .	84
Qualitätssicherung im Rahmen der Verwendung von Machine Learning . . . . .	85
Wichtige Überlegungen zum Testen . . . . .	86
Reproduzierbarkeit und Überprüfbarkeit . . . . .	87
Potenzielle Sicherheitsrisiken im Zusammenhang mit Machine Learning . . . . .	89
Adversarial Attacks . . . . .	89
Weitere Sicherheitsrisiken . . . . .	90
Das Modellrisiko eindämmen . . . . .	91
Änderungen in der Umgebung . . . . .	91
Wechselwirkungen zwischen Modellen . . . . .	92
Fehlverhalten von Modellen . . . . .	93
Abschließende Überlegungen . . . . .	94
<b>6 Deployment in die Produktivumgebung . . . . .</b>	<b>95</b>
CI/CD-Pipelines. . . . .	95
ML-Artefakte bauen . . . . .	97
Was beinhaltet ein ML-Artefakt? . . . . .	97
Die Testpipeline . . . . .	98
Deployment-Strategien . . . . .	99
Varianten des Modell-Deployments . . . . .	100
Überlegungen beim Überführen von Modellen in die Produktivumgebung . . . . .	100
Wartung von Modellen im Produktivbetrieb . . . . .	102
Containerisierung . . . . .	102
Deployments skalieren . . . . .	104
Anforderungen und Herausforderungen . . . . .	106
Abschließende Überlegungen . . . . .	107
<b>7 Monitoring und Feedback-Schleife . . . . .</b>	<b>109</b>
Wie häufig sollten Modelle neu trainiert werden? . . . . .	110
Leistungsabfall von Modellen überwachen . . . . .	113
Bewertung auf Basis der Ground Truth . . . . .	113
Abweichungen in den Eingabedaten erkennen (Input-Drift-Detection) . . . . .	116

Drift-Erkennung in der Praxis . . . . .	118
Mögliche Ursachen für systematische Abweichungen in den Daten . . . . .	118
Methoden zur Erkennung systematischer Abweichungen in den Eingabedaten . . . . .	119
Die Feedback-Schleife . . . . .	121
Logging-System . . . . .	122
Modelle evaluieren . . . . .	123
Evaluierung während des Produktivbetriebs . . . . .	126
Abschließende Überlegungen . . . . .	130
<b>8 Modell-Governance . . . . .</b>	<b>131</b>
Wer entscheidet, wie die Governance des Unternehmens aussieht? . . .	131
Anpassung der Governance an das Risikoniveau . . . . .	133
Aktuelle Regulierungen als Treiber der MLOps-Governance . . . . .	134
Gesetzliche Richtlinien für die US-Pharmaindustrie: GxP . . . . .	135
Regulierung des Modellrisikomanagements in der Finanzbranche . . . . .	135
Datenschutzbestimmungen gemäß DSGVO und CCPA . . . . .	136
Die nächste Welle an KI-spezifischen Regulierungen . . . . .	137
Die Entstehung einer verantwortungsvollen KI (Responsible AI) . . . . .	139
Schlüsselelemente von Responsible AI . . . . .	140
1. Element: Daten . . . . .	140
2. Element: Bias . . . . .	140
3. Element: Inklusivität . . . . .	142
4. Element: Modellmanagement im großen Maßstab . . . . .	143
5. Element: Governance . . . . .	143
Eine Vorlage für MLOps-Governance . . . . .	144
1. Schritt: Verstehen und Kategorisieren der Analytics- Anwendungsfälle . . . . .	145
2. Schritt: Eine ethische Grundhaltung einnehmen . . . . .	145
3. Schritt: Verantwortlichkeiten festlegen . . . . .	146
4. Schritt: Richtlinien für die Governance aufstellen . . . . .	147
5. Schritt: Einbinden von Richtlinien in den MLOps-Prozess . . . . .	149
6. Schritt: Werkzeuge für das zentrale Governance-Management auswählen . . . . .	150
7. Schritt: Einbinden und Schulen . . . . .	151
8. Schritt: Überwachen und Optimieren . . . . .	152
Abschließende Überlegungen . . . . .	153

---

## Teil III MLOps-Anwendungsfälle aus der Praxis

<b>9 MLOps in der Praxis: Kreditrisikomanagement bei der Vergabe von Verbraucherkrediten</b> . . . . .	<b>157</b>
Hintergründe des geschäftlichen Anwendungsfalls . . . . .	157
Modellentwicklung . . . . .	158
Überlegungen zu Bias in Modellen . . . . .	159
Produktionsvorbereitung . . . . .	160
Deployment in die Produktivumgebung . . . . .	161
Abschließende Überlegungen . . . . .	161
<b>10 MLOps in der Praxis: Empfehlungssysteme im Marketing</b> . . . . .	<b>163</b>
Empfehlungssysteme im Wandel der Zeit . . . . .	163
Die Rolle von Machine Learning . . . . .	164
Push- oder Pull-Empfehlungen? . . . . .	164
Datenaufbereitung . . . . .	165
Experimente konzipieren und verwalten . . . . .	166
Training und Deployment von Modellen . . . . .	167
Skalierbarkeit und Anpassungsmöglichkeiten . . . . .	168
Monitoring- und Retraining-Strategie . . . . .	168
Auswertung der Anfragen in Echtzeit (Real-Time-Scoring) . . . . .	169
Möglichkeit, das Empfehlungssystem ein- oder auszuschalten . . . . .	169
Aufbau der Pipeline und Deployment-Strategie . . . . .	169
Monitoring und Feedback . . . . .	171
Modelle neu trainieren (Retraining) . . . . .	171
Modelle aktualisieren . . . . .	171
Über Nacht laufen und tagsüber ruhen lassen . . . . .	172
Möglichkeiten zur manuellen Anpassung von Modellen . . . . .	172
Möglichkeit der automatischen Verwaltung von Modellversionen . . . . .	173
Die Qualität des Modells überwachen . . . . .	173
Abschließende Überlegungen . . . . .	174
<b>11 MLOps in der Praxis: die Verbrauchsprognose am Beispiel der Lastprognose</b> . . . . .	<b>177</b>
Stromversorgungssysteme . . . . .	177
Datenerhebung . . . . .	179
Vom Anwendungsfall abhängig: Machine Learning verwenden oder nicht? . . . . .	181
Räumliche und zeitliche Differenzierung . . . . .	182

Umsetzung .....	183
Modellentwicklung.....	184
Deployment .....	186
Monitoring .....	187
Abschließende Überlegungen.....	188
<b>Index.....</b>	<b>189</b>