

Inhaltsverzeichnis

Abkürzungsverzeichnis	17
Einleitung	21
A. Problemaufriss und Untersuchungsgegenstand	21
B. Gang der Darstellung	24
Erster Teil: Herausforderungen der KI für Recht und Regulierung	25
Erstes Kapitel: Technische Grundlagen	25
A. Terminologie	25
I. Begriffsgenese	25
II. Definitionsansätze	27
III. KI im Rechtssinne	32
IV. Verzicht auf Arbeitsdefinition	34
B. Stand der Technik	35
I. Starke und schwache KI	36
II. KI-Methoden und -Techniken	37
1. Symbolische und statistische KI	37
2. Maschinelles Lernen als Schlüsseltechnologie	38
a) Funktionsweise und Komponenten	40
b) Lernarten	43
III. Technische Ausgestaltungsmöglichkeiten	46
1. Datenintensivität	47
2. Änderbarkeit und Adaptivität	48
3. White-Box- und Black-Box-Modelle	50
C. Entwicklungs- und Integrationsprozess eines ML-basierten Systems	53
I. Konzeption	54
II. Datenmanagement	54
1. Datenmenge und -zusammensetzung	55
2. Datenqualität	56

3. Datenaufteilung	58
III. Modellauswahl	58
IV. Modellentwicklung	59
1. Allgemeines	59
2. Training künstlicher neuronaler Netze	60
3. Over- und Underfitting	61
V. Modellvalidierung und Evaluation	63
VI. Integration	66
VII. Anwendungsbeispiel aus der Medizin	67
VIII. Fazit	68
 Zweites Kapitel: KI als Gegenstand rechtlicher Betrachtung	 69
A. Kritische KI-Charakteristika aus rechtlicher Perspektive	69
I. Fehlerbehaftete und verzerrte Daten	69
II. KI-Systeme als „Blackbox“	70
1. Gefahren von Scheinkorrelationen	72
2. Berücksichtigung von Transparenzgraden und XAI-Methoden	73
III. Komplexität und Interkonnektivität	74
IV. Änderbarkeit im Betrieb	75
V. Autonomie	76
1. Autonomiegrade eines KI-Systems	76
2. Autonomiegrade in der Medizin	77
B. Problemdimensionen und Folgerungen	78
 Drittes Kapitel: Grundfragen der Regulierung	 81
A. Regulierungsdiskurs im Überblick	81
I. EU	82
1. Strategie „Künstliche Intelligenz für Europa“	83
2. Ethik-Leitlinie für eine vertrauenswürdige KI	84
3. Weißbuch zur Künstlichen Intelligenz	86
II. Deutschland	88
1. KI-Strategie der Bundesregierung	89
2. Gutachten der Datenethikkommission	89
3. Enquete-Kommission des Bundestags	90
III. U.S. Food and Drug Administration (FDA)	91

IV. Selbstregulierung durch KI-Standards und Normen	93
1. Allgemeine Initiativen	93
2. Initiativen aus dem Medizinproduktesektor	95
B. „Innovationsermöglichungsrecht“ als regulatorisches Leitbild	96
C. Metaanalyse des derzeitigen Rechtsrahmens	99
I. Regelungsstruktur und -ziele der MPVO und DSGVO	100
II. Offenheit der Normen	101
III. Technologienutralität	103
IV. Regulierung des gesamten Produktlebenszyklus	103
V. Zwischenbilanz und erste Einschätzung	105
 Zweiter Teil: Status Quo – Rechtliche Rahmenbedingungen für intelligente Medizinprodukte	 107
 Erstes Kapitel: Medizinproduktrechtliche Beurteilung	 109
A. Medizinproduktrechtliche Anforderungen an herkömmliche Software	110
I. Qualifizierung	110
1. Begriffsbestimmung der Software und Einordnung als Medizinprodukt	110
2. Zweckbestimmung	112
3. Hauptwirkung	114
II. Klassifizierung	115
1. Softwarespezifische Klassifizierungsregel	116
a) Drohende Ausuferung durch Berücksichtigung entfernter Folgen	117
b) Ansätze zur Eingrenzung der Regel	118
(1) Auslegung	118
(2) Orientierung an der IMDRF-Risikoklassifizierung	120
2. Zwischenfazit	121
III. Konformitätsbewertung	121
1. Grundlegende Sicherheits- und Leistungsanforderungen	122
2. Softwarespezifische Anforderungen	123
3. Konkretisierung durch technische Normen	124

IV. Zwischenfazit zu den Anforderungen an herkömmliche Software	124
B. Statische KI-Systeme	124
I. Qualifizierung	125
1. Maschinelles Lernen als „Medical Device Software“	125
2. „Vorhersage“, „Prognose“ und „Diagnose“ i.S.d. MPVO	126
3. Konkretisierungsbedarf des Software-Begriffs?	128
4. Zwischenfazit	129
II. Klassifizierung	130
1. Modellarchitektur	130
2. Art des Outputs	131
3. Korrelationen und stochastische Fehler	131
4. Blackbox	132
5. Zwischenfazit	132
III. Konformitätsbewertung	133
1. Gesetzliche Anforderungen	133
a) Blackbox – Transparenz, Interpretierbarkeit und Erklärbarkeit	134
b) Performanz und Datenqualität	136
c) Diskriminierung durch Verzerrungen	137
d) IT-Sicherheit und Robustheit	138
2. Untergesetzliche Anforderungen – Ein Rück- und Ausblick	140
IV. Zwischenfazit zu statischen KI-Systemen	141
C. Kontinuierlich lernende KI-Systeme	142
I. Qualifizierung	142
1. Phase vor Inverkehrbringen	143
2. Erstmalige medizinische Zweckerfüllung nach Inverkehrbringen	143
a) Vorfrage: Technische Realisierbarkeit	143
b) Regulatorische und praktische Konsequenzen	144
3. Zwischenfazit	145
II. Klassifizierung	145
1. Änderbarkeit und Adaptivität als Risikoerhöhung?	146
2. Re-Klassifizierung bei Änderungen?	146
a) Relevante Änderungen	146
b) Regulatorische Konsequenzen unter der MPVO	147

c) Zwischenfazit	148
III. Konformitätsbewertung	148
1. Regulatorischer Status Quo: Produktänderungen unter der MPVO	149
a) Regulatorische Vorgaben	149
b) Anwendbarkeit auf intelligente Medizinprodukte	150
2. Konsequenzen und ausgewählte Lösungsvorschläge	152
a) Offline-Learning	152
b) Software-Limitierungen	153
c) Antizipierte Konformitätsbewertung	153
3. Zwischenfazit	155
IV. Produktidentifikation	155
V. Herstellerwechsel?	156
1. Herstellereigenschaft und Pflichten des Herstellers	156
2. Nachträgliche Änderungen an einem Medizinprodukt	157
a) Änderungen durch den Anwender bzw. Betreiber	157
b) Autonome Weiterentwicklung	158
c) Zwischenfazit	159
3. Erstmalige Qualifizierung als Medizinprodukt durch Änderungen	159
a) Änderungen durch den Anwender bzw. Betreiber	159
b) Autonome Weiterentwicklung	161
c) Zwischenfazit	162
VI. Zwischenfazit zu kontinuierlich lernenden KI-Systemen	162
D. Zusammenfassung der Ergebnisse zum medizinprodukterechtlichen Rahmen	162
Zweites Kapitel: Datenschutzrechtliche Beurteilung	165
A. Intelligente Medizinprodukte im Anwendungsbereich der DSGVO	166
I. Anonymitätsrisiken im KI-Kontext	167
II. Beurteilungsmaßstab für einen Personenbezug	169
1. Rechtslage unter der DSRL	171
2. Kriterien zur Feststellung der Identifizierbarkeit unter der DSGVO	171
a) Berücksichtigung illegaler Mitteleinsätze	172

b) Zurechnungsmaßstab für Mittel „einer anderen Person“	173
c) Zwischenfazit und Rekonstruktion der Kriterien	174
III. Personenbezug von Trainings-, Validierungs- und Testdaten	175
IV. Personenbezug von ML-Modellen	177
1. Grundsatz	177
2. Ausnahmen	178
3. Faktoren zur Bestimmung personenbezogenen Modellinhalts	180
a) Wissenszurechnung in Hacking-Szenarien	181
b) Berücksichtigung modellspezifischer Faktoren bei der Wahrscheinlichkeitsprognose	182
(1) Modellwissen und Zugriffsrechte	182
(2) Robustheit der Modellarchitektur	183
(3) Trainingsumgebung	184
c) Zwischenfazit	185
V. Compliance-Strategien zur Reduzierung von De-Anonymisierungsrisiken	185
1. Integrierung geeigneter technischer Maßnahmen	186
2. Generelle Limitation datenschutzfreundlicher Prozesse	187
3. Konsequenzen	188
B. Technische und organisatorische Maßnahmen	188
I. Datenschutzfreundliche Voreinstellung	189
1. Datenmanagement	189
2. Privacy-Enhancing Technologies (PETs)	190
3. Modellauswahl und „Erklärbare KI“	191
4. Ort des KI-Einsatzes	192
II. Sicherheit der Verarbeitung	192
III. Fazit	195
C. Vereinbarkeit mit datenschutzrechtlichen Grundsätzen	195
I. Zweckbindungsgrundsatz	195
1. Allgemeine Präzisionsanforderungen der Zweckfestlegung	197
2. Präzisionsanforderungen bei der Modellentwicklung	199
3. Präzisionsanforderungen bei der Modellanwendung	200
4. Zwischenfazit	201

II. Datenminimierungsgrundsatz	201
1. Allgemeine Anforderungen	201
2. Datenintensive ML-Modelle	202
3. Zwischenfazit	203
III. Transparenzgrundsatz	203
1. Allgemeine Anforderungen	204
2. Herausforderungen	205
3. Zwischenfazit	206
IV. Datenrichtigkeitsgrundsatz	206
1. Entwicklungsphase – Richtigkeit und Aktualität von Trainings, Validierungs- und Testdaten	207
2. Anwendungsphase – Richtigkeit und Aktualität von Input- und Outputdaten	208
a) „Richtigkeit“ von Prognosen	209
b) Beurteilung der Richtigkeit des Outputs bei Blackbox-Modellen	211
V. Zwischenfazit	211
D. Rechtsgrundlagen für die Datenverarbeitung durch intelligente Medizinprodukte	212
I. Verarbeitung von besonderen Kategorien personenbezogener Daten	212
1. Gesundheitsdaten	213
2. Genetische Daten	213
3. Biometrische Daten	214
II. Rechtsgrundlagen für die Entwicklung intelligenter Medizinprodukte	214
1. Einwilligung	215
2. Behandlungsvertrag	216
3. Statistische Zwecke	217
4. Zwischenfazit	218
III. Rechtsgrundlagen für die Anwendung intelligenter Medizinprodukte	218
1. Statische KI-Systeme	218
a) Einwilligung	218
b) Medizinische Diagnostik	219
2. Kontinuierlich lernende KI-Systeme	221

E. Automatisierte Entscheidungsfindung durch intelligente Medizinprodukte	223
I. Rechtsnatur	224
II. Regelungsgehalt	227
1. Automatisierte Entscheidung	228
2. Ausschließlichkeit automatisierter Entscheidung	230
3. Rechtliche Wirkung oder ähnlich erhebliche Beeinträchtigungen	233
III. Intelligente Medizinprodukte als ADM-Systeme?	234
IV. Regelungsdefizit?	235
V. Innovationsfeindliche Wirkung	236
VI. Fazit	238
F. Betroffenenrechte beim Einsatz intelligenter Medizinprodukte	239
I. Identifizierbarkeit als Grundvoraussetzung	239
II. Informations- und Auskunftspflichten	241
1. Erweiterte Informations- und Auskunftspflichten	241
a) Umfang der Pflichten	242
(1) Erklärungsinhalt	243
(2) Erklärungstiefe	246
(3) Zwischenfazit	248
b) Transparenzmaßstab für intelligente Medizinprodukte	249
c) Zwischenfazit zur Transparenz	250
2. Recht auf Erklärung als „angemessene Maßnahme“ i.S.d. Art. 22 Abs. 3 DSGVO	251
3. Fazit	253
III. Recht auf Berichtigung	253
IV. Recht auf Löschung	254
1. Löschung einzelner Datenpunkte aus dem ML-Modell	255
2. Ausnahmen und Compliance-Strategien für medizinische Kontexte	255
V. Fazit zu den Betroffenenrechten	257
G. Datenschutzfolgenabschätzung	257
H. Zusammenfassung der Ergebnisse zum datenschutzrechtlichen Rahmen	259

Drittes Kapitel: Evaluation des Rechtsrahmens <i>de lege lata</i> und <i>de lege ferenda</i>	261
A. Ausgangsbefund	261
B. Anpassungs- und Ergänzungsbedarf	263
I. Antizipiertes Konformitätsbewertungsverfahren	263
II. Schaffung abgrenzbarer Verantwortungsbereiche und Einführung weiterer Akteure	264
III. Datenmanagement	266
1. Zugang zu Trainings-, Validierungs- und Testdaten	266
a) Schaffung gesetzlicher Privilegierungen	267
b) Schaffung gesetzlicher Vermutungsregeln bei Anonymitätsrisiken	268
2. Umgang mit Trainings-, Validierungs- und Testdaten	268
IV. Schaffung zusätzlicher Pflichten für ML-Prozesse	270
1. Dokumentationspflichten	271
2. Zugangspflichten	271
V. Transparenzanforderungen	272
1. Bestehende Rechtslage	273
2. Erweiterungen	274
VI. Menschliche Aufsicht	274
C. Folgerungen und Folgefragen	275
Dritter Teil: Perspektiven der europäischen KI-Verordnung	279
A. Hintergrund	279
B. Regelungsarchitektur	281
C. Wesentlicher Regelungsinhalt	283
I. Anwendungsbereich	284
II. Verbot bei unannehmbaren Risiken	284
III. Hochrisiko-KI-Systeme	285
1. Materielle Anforderungen an die Marktzulassung	285
2. Antizipiertes Konformitätsbewertungsverfahren	286
3. Nachweispflichten	287
IV. Durchsetzung und Kontrolle	287
V. Maßnahmen zur Innovationsförderung	288

D. Kritische Analyse der Auswirkungen auf intelligente Medizinprodukte	289
I. Zusammenspiel des KI-VO-E mit der MPVO	289
1. Überregulierung durch zu weite KI-Definition	289
2. Terminologische Divergenzen	292
3. Pauschale Einstufung als Hochrisiko-KI-System	293
4. Gefahr der Doppelregulierung	294
a) Grundlegende Anforderungen für Hochrisiko-KI-Systeme	295
b) Marktüberwachung	297
c) Zwischenfazit	298
5. Praktische Umsetzungsschwierigkeiten	299
a) Anforderungen an die Daten und Daten-Governance	299
(1) Fehlerfreiheit und Vollständigkeit	299
(2) Verzerrungen	300
b) Transparenzanforderungen	301
c) Anforderungen an die menschliche Aufsicht	302
d) Konformitätsbewertung durch Benannte Stellen nach der MPVO	304
6. Inkongruente Pflichten der Wirtschaftsakteure	305
II. Zusammenspiel des KI-VO-E mit der DSGVO	307
1. Unklares Verhältnis	307
2. Ergänzungen um KI-spezifische Rechtsgrundlagen	308
3. Extensive Zugriffsrechte der Marktüberwachungsbehörden	310
4. Inkongruente Pflichten der Wirtschaftsakteure	311
III. Dreidimensionale Regulierungsdynamik	312
E. Zwischenbilanz zum KI-VO-E	313
F. Ausblick	316
Literaturverzeichnis	319