

Inhaltsverzeichnis

Vorwort zur dritten Auflage	V
Abkürzungsverzeichnis	XIX
Autorenverzeichnis	XXVII
Bearbeiterverzeichnis	XXXI

Kapitel 1 Einführung

§ 1 Industrie 4.0 und Industrial Internet of Things	1
I. Einleitung	3
II. Stand der Nutzung von IoT	6
III. Konnektivität	9
1. Kabelgebundene Konnektivität	9
2. Funktechnologien im unlizenzierten Spektrum	10
3. Funktechnologien im lizenzierten Spektrum	11
4. Nummernressourcen	13
5. eSIM	14
IV. Cloud-Infrastrukturen und darauf aufsetzende IoT-Plattformen	15
1. Verschiedene Formen von Cloud-Infrastrukturen	15
2. IoT-Plattformen	19
V. Daten und Datenaustausch	20
1. Standards und Protokolle für den Datenaustausch	21
2. Digitaler Zwilling und Verwaltungsschale	23
3. Datenräume	24
VI. Ausgewählte Anwendungen von Industrie 4.0 und IoT	26
1. Anwendungsbeispiele für mehr Transparenz im Produktionsprozess ...	26
2. Anwendungen mit künstlicher Intelligenz	27
3. Robotik	30

Kapitel 2 Typische Rechtsfragen

§ 2 Schutz von maschinengenerierten Daten	35
I. Einführung	37
1. Begriffsbestimmung	40
2. Abgrenzung zum Datenschutzrecht	41
II. Schutz maschinengenerierter Daten – an den Grenzen der Gesetze	42
1. Schutz durch IP-Rechte	43
2. Schutz maschinengenerierter Daten als Geschäftsgeheimnis	52
3. Lauterkeitsrechtlicher Schutz von maschinengenerierten Daten	63
4. Kein besitzrechtlicher Schutz von maschinengenerierten Daten	64
5. Strafrechtliche und kapitalmarktrechtliche Ansätze	65
III. Maschinengenerierte Daten – Versuche der Grenzverschiebung	67
1. Scheitern von sachenrechtlichen Begründungen	67
2. Vorschlag eines „Rechts des Datenerzeugers“/„Datenherstellerrechts“ .	69
3. EU-Data Act: Ablehnung neuer Ausschließlichkeitsrechte	70
IV. Begrenzung des Schutzes durch den EU Data Act	71
1. Sachlicher Anwendungsbereich	71
2. Ausschluss des Datenbankherstellerrechts, Art. 43 DA	74
3. Reduktion des Geheimnisschutzes	76

VII

Inhaltsverzeichnis

V. Vertragliche Gestaltungsmöglichkeiten	87
1. Kategorisierung von maschinengenerierten Daten	88
2. Vereinbarungen über Datennutzungen	90
§ 3 Kooperation bei Forschung und Entwicklung	96
I. Erscheinungsformen kooperativer F98	
1. Unterscheidung nach Dimensionen	99
2. Unterscheidung nach der Bestimmbarkeit des Teilnehmerkreises	100
II. Vertragsgestaltung	100
1. Semi-offene Innovationsprozesse	101
2. Offene Innovationsprozesse	112
III. Kartellrecht	115
IV. Ausblick	118
§ 4 Haftungsfragen bei vernetzten und autonomen Systemen	120
I. Einführung	122
II. Vertragliche Haftung	123
III. Produkt- und Produzentenhaftung	125
1. Die deliktsrechtliche Produzentenhaftung	125
2. Produkthaftung nach dem Produkthaftungsgesetz	131
IV. Deliktsrechtliche Haftung im Übrigen	136
1. Haftung gem. § 823 Abs. 1 BGB	136
2. Haftung gem. § 823 Abs. 2 BGB	136
V. Haftungsumfang	137
VI. Besondere Probleme der gesetzlichen Haftungstatbestände im Zusammen- hang mit IoT und Industrie 4.0	138
1. Neue Produktrisiken durch neue Funktionen	138
2. Produktsicherheit und IT-Sicherheit – Haftung für Schäden durch Cyber-Angriffe	139
3. Apps und Software	148
4. Das Nichtfunktionieren als Produktfehler	149
5. Bestimmung des Herstellers beim Einsatz innovativer Produktionstechnologien	150
6. Abgrenzung von Verantwortungsbereichen in der Wertschöpfungskette	151
VII. Haftung und öffentlich-rechtliche Verantwortung für KI	152
1. Die zivilrechtliche Haftung für Künstliche Intelligenz	156
2. Die KI-VO	159
3. Der Entwurf einer KI-Haftungsrichtlinie	161
VIII. Betreiber-/Benutzerhaftung	162
1. Haftung nach dem HaftPflG	163
2. Kfz-Halterhaftung	163
3. Deliktische Haftung des Benutzers	163
4. Haftungsrechtliche Berücksichtigung des Einsatzes von automatisierten Systemen	164
IX. Umfang der Schadensersatzansprüche	164
X. Möglichkeiten der Haftungsbeschränkung für Hersteller	164
XI. Zusammenfassung der haftungsrechtlichen Herausforderungen	165
§ 5 Anforderungen des Telekommunikationsrechts	167
I. Anwendbarkeit der Regelungen des Telekommunikationsgesetzes	169
1. Geschäftsmodelle und regulatorische Anknüpfungspunkte	169
2. Connectivity Service Provider	170
3. IoT Service Provider	175
4. IoT User	176

5. Fallbeispiele	178
6. Zwischenergebnis	179
II. Meldung und Aufsicht durch die Bundesnetzagentur	180
III. Kundenschutz	180
1. Anwendbarkeit der kundenschützenden Regelungen auf Verbraucher und Unternehmer	181
2. Bündelangebote	183
3. Vertragliche Informationspflichten und Vertragsdauer	184
4. Auswirkung der Regelungen zur sog. Endgerätefreiheit	185
5. Netzneutralität	186
6. Haftung für Vermögensschäden	187
7. Fragen der Abrechnung	188
8. Sperre von Nutzern	190
IV. Frequenzen	192
1. Hintergrund	192
2. 5G-Spektrum	193
3. Frequenzzuteilung	194
4. Anzeigepflicht, Kosten und Widerruf	197
5. Zuteilungsgebiet	198
6. Netzzugang	201
V. Nummerierung und Nummernnutzung	202
1. (Ruf-)Nummern für IoT Dienste	202
2. Adressierung von ortsfesten IoT Endgeräten	206
3. Adressierung von mobilen IoT Endgeräten	207
4. Zuteilung von Nummern durch die Bundesnetzagentur	209
5. Zuteilung von IP-Adressen	211
6. Zuteilung von IMSI	212
7. Anbieterwechsel und Rufnummernportierung bei IoT Diensten	212
VI. Fernmeldegeheimnis und Datenschutz	214
1. Entwicklung des TK-Datenschutzes	214
2. DS-GVO und TK-Datenschutz	215
3. Fernmeldegeheimnis bei IoT Diensten	217
4. Telekommunikationsdatenschutz	219
VII. Öffentliche Sicherheit	222
1. In der Regel keine Notrufverpflichtung bei IoT Anwendungen	222
2. eCall Verpflichtung	224
3. Schutz der Systeme und Daten bei IoT Anwendungen	225
4. Telekommunikationsbevorrechtigung für IoT User und IoT End-User	231
5. Behördenbeauskunftung und Überwachungsmaßnahmen	232
VIII. Roaming von IoT Anwendungen	238
1. Hintergrund des Roamings bei IoT Anwendungen	238
2. Anwendbarkeit der Roaming-Verordnung auf IoT Anwendungen	239
3. Roamingentgelte	239
IX. Ansprüche und Schlichtung	239
1. Ansprüche von Kunden, Verbraucherverbänden und Mitbewerbern	239
2. Schlichtung	240
X. Übernahme der Verpflichtungen durch den Connectivity Service Provider	240
XI. Zusammenfassung Telekommunikationsrecht	242
§ 6 Datenschutz und IT-Sicherheit	244
I. Einführung	246
1. Datenschutz	246
2. IT-Sicherheit	246

Inhaltsverzeichnis

II. Datenschutz	247
1. Systematik des Datenschutzrechts	248
2. Personenbezogene Daten	250
3. Räumlicher Anwendungsbereich datenschutzrechtlicher Regelungen ..	254
4. Datenschutzrechtliche Verantwortlichkeiten	258
5. Rechtmäßigkeit der Datenverarbeitung	261
6. Informationspflichten, Rechte der Betroffenen	264
7. Technische und organisatorische Datenschutzmaßnahmen	271
8. Folgen bei Datenschutzverstößen	277
III. IT-Sicherheit	286
1. Bedrohungs- und Angriffsszenarien	286
2. Ordnungsrecht	288
3. IT-Sicherheit vs. Datenschutz – Erfordernis eines Ausgleichs	301
§ 7 Kartellrechtlicher Rahmen	303
I. Einführung	305
II. Der Kartellrechtsrahmen im Überblick	308
1. Kartellrechtliche Grundsätze	308
2. Marktdefinition als Ausgangspunkt jeder wettbewerblichen Beurteilung	309
3. Kartellverbot und Gruppen- oder Einzelfreistellung	310
4. Missbrauchsverbot	312
5. Fusionskontrolle	313
6. Exkurs: kartellrechtsnahe Regulierung von Plattformen und	
Datenzugang	316
III. Einzelfragen	318
1. Kartellrechtliche Erfassung von Plattform-Geschäftsmodellen	318
2. Missbrauch der Intermediationsmacht von Plattformen	324
3. Tipping als spezifischer Missbrauchs-/Gefährdungstatbestand	
(Monopolisierungsverbot)	324
4. Missbrauch durch Unternehmen mit überragender marktübergreifender	
Bedeutung für den Wettbewerb	325
5. Marktmacht und Daten	326
6. Probleme des Kartellverbotes	333
7. Technische Standards/Normen	338
IV. Zusammenfassende Bewertung	341
§ 8 Arbeitsrecht – Realität und Herausforderungen	342
I. Einführung	344
II. Arbeitsrecht 4.0? – Realität und Anpassungsbedarf	345
1. Andere Arbeitsformen – Plattformökonomie und „Crowdworking“ ...	346
2. Auswirkungen auf den Arbeitsort	349
3. Arbeitszeitfragen	359
4. Spielarten künstlicher Intelligenz in der Arbeitswelt	363
5. Kündigungsgrund „Digitalisierung“ – Arbeitsplatzverlust infolge von	
Digitalisierung und Automatisierung	366
6. Die Rolle des Betriebsrats in der Industrie 4.0	368
7. Arbeitsschutz und Gesundheitsschutz in der Industrie 4.0	374
8. Beschäftigtendatenschutz und Arbeitnehmerkontrolle	376
9. Arbeitskampf und Gewerkschaftsarbeit in der Industrie 4.0	382
§ 9 Gesellschaftsrecht	384
I. Problemstellung	384
II. Charakteristika einer Personengesellschaft und Abgrenzungsfragen	385
1. Vorliegen einer Personengesellschaft	386

2. Erscheinungsformen von Personengesellschaften	388
3. Abgrenzung von anderen Vertragstypen	392
III. Beispiele von (regelungsbedürftigen oder nunmehr gesetzlich vorgegebenen) bemerkenswerten Inhalten vor Beginn eines Projekts	394
1. Eigentumsverhältnisse und Nutzungsrechte	395
2. Höchstpersönliche Gesellschafterstellung; Übertragbarkeit von Anteilen	395
3. Ausscheiden eines Gesellschafters	396
IV. Personengesellschaften im internationalen Kontext	396
§ 10 Strafrecht	399
I. Moderne Entwicklungen, tradiertes Strafrecht?	400
II. Angriffe unmittelbar gegen das System	401
1. Angriffe auf das IoT als Datenveränderung iSd § 303a StGB	402
2. Angriffe auf das IoT als Computersabotage iSd § 303b StGB	407
3. Angriffe auf das IoT de lege lata und de lege ferenda	411
III. Angriffe unmittelbar gegen die Daten	412
1. Angriffe auf die Daten als Ausspähen von Daten iSd § 202a StGB	412
2. Angriffe auf die Daten als Abfangen von Daten iSd § 202b StGB	415
3. Vorbereiten des Ausspähens und Abfangens der Daten iSd § 202c StGB	416
4. Anschließende Datenhehlerei iSd § 202d StGB	417
5. Angriffe auf die Daten als Straftat iSd § 42 BDSG	418
6. Angriffe auf die Daten de lege lata und de lege ferenda	419
IV. Zukunft des Strafrechts der Dinge	420
§ 11 Zivilprozessrecht	421
I. Einführung	422
II. Zivilprozessuale Besonderheiten bei IoT und Industrie 4.0-Sachverhalten ..	422
1. Typische Prozesskonstellationen	422
2. Zuständigkeitsfragen und internationales Privatrecht	423
3. Bestimmung der Passivlegitimation und Beteiligung mehrerer Parteien	427
III. Technologische Herausforderungen und ihre Auswirkungen auf das Zivilverfahren	429
1. Beweisschwierigkeiten beim Einsatz von IoT Geräten und KI-Systemen	429
2. Prozessuale Anforderungen bei der Klärung technischer Sachverhalte ..	431
3. Beweisführung mit Daten von IoT-Gegenständen	433
4. Bestimmung des Beweiswerts von Daten aus IoT Geräten	437
IV. Checkliste für Klageverfahren mit Bezug zu IoT-Geräten	438
V. Ausblick: Einsatz technischer Hilfsmittel im Zivilprozess	439

Kapitel 3: Besonderheiten bei Vertragsschluss und -gestaltung

§ 12 Vertragsschluss beim IoT Rechtsgeschäft	441
I. Einführung und Fallbeispiel	442
II. Allgemeine Grundzüge des Vertragsschlusses	444
1. Prinzipien	444
2. Der Softwareagent im Rechtsverkehr	450
3. Zusammenfassung	461
III. Internet of Things und Allgemeine Geschäftsbedingungen	462
1. Ausgangspunkt: Strenge des deutschen AGB-Rechts	464
2. Interessenslage für Hersteller und Betreiber von M2M-Kommunikationssystemen und Softwareagenten	470
3. Handlungsbedarf für den Gesetzgeber	470
IV. Praxistipps	471

Inhaltsverzeichnis

§ 13 Besonderheiten bei Verbraucherverträgen 472

 I. Die Anwendbarkeit der fernabsatzrechtlichen Regelungen 474

 1. IoT als Teil der besonderen Betriebsformen, §§ 312 ff. BGB 474

 2. Bereichsausnahmen 478

 3. Außerhalb von Geschäftsräumen geschlossener Vertrag oder Fernabsatzvertrag 480

 4. Vertrag im elektronischen Geschäftsverkehr 482

 II. Informationspflichten bei Verbraucherverträgen 482

 1. Vorvertragliche Informationspflicht 482

 2. Nachvertragliche Informationspflicht 486

 3. Einzelne Informationspflichten aus Art. 246a § 1 EGBGB 486

 4. Weitere Pflichten im elektronischen Geschäftsverkehr 493

 III. Gestaltung von IoT-Modellen in der Praxis 496

 1. Verwendete Modelle („dash button“, „amazon echo“ et al.) 496

 2. Anforderungen an die Gestaltung von IoT-Geschäftsmodellen de lege lata 498

 3. Zusammenfassung und Ausblick 498

§ 14 Vertragstypen und Herausforderungen der Vertragsgestaltung 500

 I. Einführung 501

 II. Vertragsgegenstand 504

 1. Arten von Verträgen 504

 2. Vertragsstruktur 505

 3. Vertragstypologische Einordnung 506

 III. Hauptleistungspflichten 507

 1. Leistungsbeschreibung 507

 2. Wesentliche Hauptleistungen 508

 IV. Allgemeine Beschaffenheitsvereinbarungen 528

 1. Software ist nie fehlerfrei 529

 2. IT-Sicherheit 529

 3. Frei von Rechten Dritter 532

 4. Sollbeschaffenheit von Daten und Informationen 532

 5. Indirekte Nutzung von Software 535

 V. Gewährleistung 537

 1. Mangelbegriff 537

 2. Mängelrechte 540

 VI. Service Level Agreements 541

 1. Qualität der Leistung 541

 2. Messung von Service Level Agreements 542

 3. Sanktionen für Service Level Agreement Verletzungen 542

 VII. Haftung 543

 1. Begriff der Haftung 544

 2. Haftungstatbestände 544

 3. Haftungsbeschränkungen 546

 VIII. Informations- und Datenschutz 547

 1. Umgang mit vertraulichen Informationen 547

 2. Umgang mit personenbezogenen Daten 547

 3. Umgang mit sonstigen Informationen 547

 IX. Zusammenfassung 550

 X. Checkliste Vertragsgestaltung 550

Kapitel 4 Besonderheiten ausgewählter Technologien

§ 15 Künstliche Intelligenz und Machine Learning	553
I. Einführung	555
1. Entstehungsgeschichte und Begrifflichkeiten	555
2. Grundlegende Funktionsweise von künstlicher Intelligenz	556
3. Einsatz von künstlicher Intelligenz	558
4. Typische rechtliche Fragestellungen	559
II. Regulatorischer Rahmen	560
1. Verordnung über künstliche Intelligenz	560
2. KI spezifische Risiken („Responsible AI“)	567
3. Folgen für die Unternehmens-Governance	571
III. Künstliche Intelligenz und Datenschutz	572
1. Personenbezug von KI-Modellen	573
2. Wahrscheinlichkeitsaussagen und der Grundsatz der Datenrichtigkeit ..	574
3. Datenschutzrechtliche Verantwortlichkeiten beim Einsatz von KI-Systemen	575
4. Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten beim Einsatz und Training von KI-Systemen	576
5. Verbot automatisierter Entscheidungen	579
6. Informationspflichten	581
7. Datenschutzfolgenabschätzung	583
IV. Künstliche Intelligenz und geistiges Eigentum	584
1. Training von KI-Systemen	584
2. Schutz von KI-Systemen	586
3. Zwischenergebnis und Ausblick	591
V. Vertragsgestaltung	591
1. Dogmatische Einordnung des Vertrags	592
2. Verantwortung für Entscheidungen	594
3. Rechte an Daten	594
VI. Checkliste für KI-Projekte	596
§ 16 Blockchain	598
I. Einführung	600
1. Hintergründe der Blockchain-Technologie	600
2. Bedeutung der Blockchain-Technologie	601
3. Geschichte der Blockchain	601
4. Arten und Funktionsweise einer Blockchain	602
5. Rechtliche Fragen der Blockchain-Nutzung	604
II. Urheberrechtliche Einordnung der Blockchain und Fragen des gewerblichen Rechtsschutzes	605
1. Allgemeines	605
2. Blockchain	605
3. Einzelne Elemente einer Blockchain	611
4. Client-Software	612
III. Datenschutzrechtliche Einordnung der Blockchain	614
1. Allgemeines	614
2. Vorliegen personenbezogener Daten	615
3. Datenschutzrechtliche Verantwortlichkeit innerhalb einer Blockchain ..	616
4. Auftragsverarbeitung innerhalb der Blockchain	619
5. Rechtmäßigkeit der Datenverarbeitung und Betroffenenrechte	619
IV. Zivilrechtliche Fragen im Zusammenhang mit der Blockchain-Technologie	622
1. Zivilrechtliche Rahmenbedingungen der Blockchain	622

Inhaltsverzeichnis

2. Haftung der Nutzer der Blockchain	622
3. Ausgestaltung der Nutzungsbedingungen	625
4. Sonstige Anforderungen	626
V. Zivilprozessuale Fragestellungen	626
1. Erkenntnisverfahren	626
2. Vollstreckungsverfahren	627
VI. Strafrechtliche Bewertung der Blockchain-Nutzung	628
1. Allgemeine Grundsätze der strafrechtlichen Verantwortlichkeit der Nutzer.	628
2. Sonderfälle	629
VII. Ausgewählte Erscheinungsformen und Einsatzgebiete	629
1. Kryptowährungen	629
2. Initial Coin Offerings	632
3. Nachverfolgbarkeit innerhalb von Lieferketten	633
4. „Blockchain Grundbuch“ und digitales Handelsregister	633
5. Non-Fungible Token (NFT)	633
§ 17 Smart Contracts	634
I. Einführung	634
II. Allgemeines	635
III. Zivilrechtliche Fragen im Zusammenhang mit Smart Contracts	636
1. Allgemeine Rahmenbedingungen	636
2. Sonderfall der „Datenweitergabevereinbarungen“	638
IV. Störungen bei der Vertragsdurchführung	639
1. Technische Limitierungen	639
2. Fehlerhafte Erklärungen	640
3. Problem der eigenmächtigen Rechtsdurchsetzung	640
V. Streitschlichtungsverfahren	641

Kapitel 5 Besonderheiten ausgewählter Branchen

§ 18 Digitalisierung des Gesundheitswesens (eHealth)	645
I. Einführung	647
1. Nutzungsmöglichkeiten	647
2. Regulatorische Aspekte	648
3. Datenschutz und Cybersecurity	649
4. Haftungsfragen	653
II. Fortschreibung der Digitalisierung durch die Gesetzgebung	653
III. gematik und Telematikinfrastruktur	656
1. gematik	656
2. Telematikinfrastruktur	657
IV. Ambulante Leistungserbringung	676
1. Digitale Technologien und Apps in der ambulanten Versorgung	676
2. Telemedizinische Leistungen in der ärztlichen Versorgung	683
3. Haftung im Bereich der ärztlichen Nutzung digitaler Technologien ...	694
4. Ausblick: Grenzüberschreitende elektronische Gesundheitsdienste und elektronischer Datenaustausch	695
V. Klinische Prüfung und Forschung	699
1. Übergreifend: Einsatz von KI im Lebenszyklus eines Arzneimittels oder Medizinproduktes – KI-Verordnung	700
2. Prominente Einsatzgebiete von digitalen Technologien	703
3. Sekundärnutzung von Gesundheitsdaten zu Forschungszwecken (EHDS; Gesundheitsdatennutzungsgesetz)	713

VI. Digitalisierung der Medizinprodukte-Branche und in der Arzneimitteltherapie	724
1. Medizinprodukte – Abgrenzungsfragen	726
2. Vorgaben nach der EU-Medizinprodukteverordnung/MDR	729
3. Datenschutzrechtliche Vorgaben	730
4. Haftungsfragen, Produkt- und Datenverantwortung	731
§ 19 Automatisiertes Fahren (Automotive)	737
I. Einführung	739
II. Begriffliche Schärfung	740
1. Nomenklatur der Bundesanstalt für Straßenwesen zur Fahrzeugautomatisierung	740
2. Achten StVG-Änderungsgesetz	741
3. Gesetz zum autonomen Fahren	743
III. Zulassungsrechtlicher Rahmen für automatisierte Fahrzeuge	746
1. Fahrzeugzulassung und -genehmigung	746
2. EU-Typgenehmigung	746
3. (Keine) Auswirkungen des Achten StVG-Änderungsgesetzes auf die Fahrzeugzulassung	751
4. Sonderzulassungsrecht des Gesetzes zum autonomen Fahren	752
IV. Haftungsrechtliche Implikationen der Fahrzeugautomatisierung entlang der Lieferkette	754
1. Haftung des Fahrzeughalters	754
2. Haftung des Fahrzeugführers	757
3. Haftung des Fahrzeugherstellers	762
V. Ausblick	769
§ 20 Digitalisierung des Energiesektors (Smart Grids)	772
I. Die Energiewende als nationales IT-Projekt	773
1. Transformation zu erneuerbaren Energien	774
2. Energieeffizienz	775
3. Digitalisierung der Energiewende	775
II. Herausforderungen und Chancen für die Energiewirtschaft	777
1. Erzeugung und Speicherung	777
2. Übertragung und Verteilung (Smart Grids)	778
3. Messwesen (Smart Metering)	778
4. Vertrieb und Marketing	779
III. Chancen und Herausforderungen für die Industrie (Verbraucher)	779
IV. Rechtlicher Rahmen	780
1. Messstellenbetriebsgesetz	780
2. Erzeugungsanlagen EEG und KWKG	791
V. Praxisbeispiele	791
1. Virtuelles Kraftwerk	791
2. Elektromobilität – Autos als Energiespeicher	792
VI. Zusammenfassung und Ausblick	793
§ 21 Digitalisierung der Versicherungswirtschaft (InsurTech)	794
I. Bestandsaufnahme und Begriffsbestimmung	794
II. Neue Technologien und neue Formen von Versicherung	799
III. Versicherungsvertrieb	803
1. Einleitung	803
2. Zulässigkeit der Versicherungsvermittlung	804
3. Zivilrechtliche Vorgaben	806

Inhaltsverzeichnis

IV. Versicherungsprodukte	811
1. Einleitung	811
2. Kfz-Versicherung (Telematik-Tarife)	814
3. Berufsunfähigkeits- und Lebensversicherung	815
4. Cyber-Versicherungen	818
§ 22 Digitalisierung der Bankenwelt (FinTech)	821
I. Einführung	823
1. Begriffsbestimmung	823
2. Wesentliche Eigenschaften von FinTech Unternehmen	824
3. Kategorisierung des FinTech Marktes	825
4. Wirtschaftliche Bedeutung und Ausblick	826
5. Verhältnis zwischen FinTech Unternehmen und traditionellen Anbietern	826
II. Europäische und deutsche Finanzaufsichtsbehörden	827
1. Europäisches System der Finanzaufsicht	827
2. Deutsches System der Finanzaufsicht	829
III. Wesentliche aufsichtsrechtliche und sonstige rechtliche Rahmenbedingungen	829
1. KWG	830
2. ZAG	838
3. Weitere relevante Vorschriften	841
4. Aktuelle rechtliche Entwicklungen	842
IV. Grenzüberschreitende Sachverhalte – Europäischer Pass	846
1. Europäischer Pass nach §§ 24a und 53b KWG	846
2. Europäischer Pass nach §§ 38 und 39 ZAG	847
3. Passive Dienstleistungsfreiheit	847
V. Beteiligung an FinTech Unternehmen mit einer Erlaubnis nach KWG bzw. ZAG	847
VI. Das Verhältnis der BaFin zu FinTech Unternehmen	849
VII. Aufsichtsrechtliche Strategien für FinTech Unternehmen	850
1. Beantragung einer Lizenz	850
2. Vermeidung aufsichtsrechtlich relevanter Tätigkeiten	851
3. Inanspruchnahme von Ausnahmetatbeständen	852
VIII. FinTech-Geschäftsmodelle	852
1. Alternative Bezahlverfahren	853
2. Currency Token (Payment Token)	856
3. Crowdfinanzierung	861
4. Crowdlending	861
5. Crowdfunding	868
6. Buy Now Pay Later	872
7. Automatisierte Finanzportfolioverwaltung und Anlageberatung (Robo Advice)	873
IX. Aktuelle FinTech Trends	877
1. Blockchain	877
2. Künstliche Intelligenz (AI)	878
3. Embedded Finance	878
4. Convenience Tech und Financial Wellbeing	878
§ 23 Unbemannte Luftfahrzeuge (Aviation)	880
I. Einführung	880
II. Arten und Rechtsgrundlagen für unbemannte Luftfahrzeuge	881
1. Einteilung der unbemannten Luftfahrzeuge nach technischen Kriterien	881
2. Europäischer und deutscher Rechtsrahmen	883

III. Rechtsfragen im Umgang mit unbemannten Luftfahrzeugen	889
1. Herstellung von unbemannten Luftfahrzeugen	889
2. Betrieb von unbemannten Luftfahrzeugen	892
3. Kennzeichnungspflicht der unbemannten Luftfahrzeugsysteme und Registrierungspflicht der Betreiber	900
4. Infrastruktur für unbemannte Luftfahrzeuge	901
5. Finanzierung von unbemannten Luftfahrzeugen	903
IV. Internationaler Vergleich der Drohnenregulierung	905
V. Ausblick in die Zukunft	907
Anhang: Vergleich Anforderungen „spezielle“ und „zulassungspflichtige“ Kategorie	909
Sachverzeichnis	913