

Rechtshandbuch der Digitalisierung

herausgegeben von

ao. Univ.-Prof. Dr. Wolfgang Zankl

Universität Wien



Wien 2021

MANZ'sche Verlags- und Universitätsbuchhandlung

Inhaltsverzeichnis

Vorwort	V
Verzeichnis der Autorinnen und Autoren	XXV
Abkürzungsverzeichnis	XXVII

Teil I Grundlagen der Digitalisierung

1. Kapitel Die Bedeutung der Digitalisierung in der Praxis und im Recht	1
I. Digital Legal Expert – neue juristische Anforderungen	1
II. Digitalisierung und Recht in Zeiten der Pandemie	2
III. Ausblick	5
2. Kapitel Grundlagen der Digitalisierung und Legal Tech	6
I. Einstieg in die Welt der Digitalisierung und Legal Tech	7
A. Definitionsversuch: Digitalisierung	7
B. Digital Thinking	7
II. Legal Tech und Buzzwords der Digitalisierung	8
A. Amaras Gesetz	8
B. Legal Tech	9
C. Juristen als Fortschrittsverhinderer?	10
D. Fakten zu bestimmten Technologien	10
1. Allgemeines zu Legal Tech	11
2. Artificial Intelligence	11
3. Natural Language Processing	12
4. Blockchain	13
5. Smart Contracts	14
6. Big Data	15
7. Chatbots	16
8. E-Discovery und TAR-Systeme	17
9. Robotic Process Automation	17
10. Low-Code-/No-Code-Technologie	17
3. Kapitel Grundlagen der Informatik und IT-Security	19
I. Einführung	19
II. Einleitung: Was ist Informatik?	21
A. Allgemeines	21
B. Kernbereiche der Informatik	21
1. Theoretische Informatik	22
2. Technische Informatik	22
3. Praktische Informatik	22
4. Angewandte Informatik	23
III. Betriebssysteme und alternative Architekturen	23
A. Betriebssystem	23
B. Alternative Architekturen	24
IV. Algorithmen und Computerprogramme	24
A. Algorithmus	24
B. Computerprogramm	25

Inhaltsverzeichnis

1. Definition	25
2. Aufbau von Computerprogrammen	26
3. Programmiersprachen	26
4. Cloud Computing	27
5. Definition	28
6. Cloud-Servicemodelle	28
V. Security als Managementfunktion	28
A. Hacker und ihre Motivation	29
B. Informationssicherheit	30
1. Warum ist Informationssicherheit von Bedeutung?	30
2. Arten von Informationswerten	31
3. Unterscheidung IT-Security und Informationssicherheit	31
4. Zusammenhang Informationssicherheit und Datenschutz	32
5. Informationssicherheitsmanagementsystem (ISMS)	33
6. ISO/IEC 27001	34
C. Awareness	35
4. Kapitel Cloud Computing	38
I. Grundlagen	38
A. Definition von Cloud Computing	38
B. Die fünf wesentlichen Merkmale eines Cloud Service	40
C. Service-Modelle	40
D. Bereitstellungsmodelle	42
E. Cloud-Only- oder Cloud-First-Strategie?	43
II. Infrastrukturen und Anwendungsgebiete	44
III. Künstliche Intelligenz und Machine Learning	45
A. Bestehende Einsatzgebiete	46
B. Aufkommende Einsatzgebiete	47
5. Kapitel Digital Leadership	48
I. Digital Leadership	48
A. Agile Führung	50
B. Generationsorientierte Führung	50
C. Virtuelle Führung	51
D. Neue Anforderungen an Führungskräfte	52
E. VOPA+-Modell	52
1. Vertrauen	53
2. Partizipative Führung	53
3. Kommunikation	54
4. Feedback	54
II. Scrum	54
A. Was ist Scrum?	54
B. Scrum Basics	55
1. Scrum-Rollen	55
a) Product Owner	55
b) Entwicklungsteam	56
c) Scrum Master	56
2. Ablauf eines Sprints	57
a) Sprint Planning	57
b) Daily Scrum	57
c) Sprint Review	57
d) Sprint Retrospektive	57
3. Artefakte	58

a) Product Backlog	58
b) Sprint Backlog	58
c) Product Increment	58
III. Fazit	58

Teil II

Digitalisierung im Privatrecht

6. Kapitel E-Commerce und Vertragsrecht	59
I. E-Commerce und E-Commerce-Recht im Allgemeinen	59
II. ABGB, GRUG und E-Commerce-Gesetz	61
A. E-Commerce-Gesetz im Überblick	61
1. Anwendungsbereich	61
2. Regelungsschwerpunkte	62
B. Vertragliche Regelungen im Einzelnen	62
1. Vertragsabschluss und vertragliche Erklärungen	62
2. Vertragsqualifikation und Vertragsinhalte	64
3. Vertragliche Informationspflichten	66
4. Vertragsstörungen	68
5. Vertragliche AGB	72
6. Übergang vertraglicher digitaler Inhalte von Todes wegen	73
III. Fernabsatzrecht	74
A. Fern- und Auswärtsgeschäfte-Gesetz – FAGG	74
1. Allgemein	75
2. Informationspflichten	76
3. Rücktrittsrecht	77
B. Fernfinanzdienstleistungsgesetz – FernFinG	79
1. Allgemein	79
2. Informationspflichten	79
3. Rücktrittsrecht	79
7. Kapitel E-Commerce und Haftungsrecht	80
I. ABGB und E-Commerce-Gesetz	81
A. Haftung	81
B. Haftungsbefreiung	83
1. Allgemein	83
2. Access-Provider	86
3. Host-Provider	87
4. Suchmaschinen	89
5. Linksetzer	92
6. Überwachungs-, Nachforschungs- und Auskunftspflichten	93
II. Hass-im-Netz-Bekämpfungsgesetz und Kommunikationsplattformengesetz	98
III. Herkunftslandprinzip	101
8. Kapitel Recht der elektronischen Signaturen	104
I. Elektronische Signaturen	105
A. Digitale und elektronische Signaturen	105
1. Technologieneutraler Ansatz	105
2. Bedeutung	105
3. Funktionalitäten	105
4. Zweck	106
5. Unterscheidungen	106
6. Signaturprodukte	106

7. Signaturerstellung und Signaturprüfung	107
B. Rechtliche Rahmenbedingungen	107
1. EU-Verordnung mit SVG und SVV	107
2. Definitionen	108
3. Innerstaatliche Konkretisierung	109
C. Qualifizierte elektronische Signatur	109
1. Elemente	109
2. Qualifiziertes Zertifikat	109
3. Qualifizierte Signaturerstellungseinheit	110
4. E-Mail-Signatur	110
5. Bestätigungsstellen	111
6. Ausstellen eines qualifizierten Zertifikats	111
7. Verzeichnis- und Widerrufsdienst	111
8. Qualifizierter VDA	112
D. Haftung des VDA	113
E. Pflichten der Signatoren	113
F. Besondere Rechtswirkungen	113
G. Signaturprüfung	115
H. Elektronisches Siegel	116
II. Elektronische Urkunden und Beweismittel	117
A. Verfahrensrecht	117
B. Nichtdiskriminierung	117
C. Qualifiziert elektronisch signierte Dokumente	117
D. Elektronisches Siegel	117
III. Notarielle Urkunden, Archivierung und Applikationen	118
A. Urkundenarchiv	118
B. Notarsignatur und Beurkundungssignatur	118
C. Beurkundungssignatur (öffentliche Form)	119
D. Beurkundungssignatur (notarielle Urkunden)	119
E. Archivierungssignatur und Archivsignatur	119
F. Signaturpraxis in Österreich	120
IV. Elektronischer Akt	121
A. Elektronisches Aktenregister	121
B. Justiz 3.0	121
9. Kapitel Legal Tech: Die elektronische Signatur im Unternehmen	122
I. Eine kleine Maßnahme mit großer Wirkung	123
A. Der lange Weg zur elektronischen Signatur	123
B. Die Bedeutung der elektronischen Signatur für Digitalisierungs-Initiativen	123
C. Menschliches, Allzumenschliches	125
D. Glossar zu elektronischen Signaturen	126
II. Elektronische Signaturen im Unternehmen – Empfehlungen	128
A. Strategie	128
B. Governance	128
C. Technisches, Allzutechnisches – was elektronische Signaturen im Unternehmen leisten	130
D. Signatur-Workflows auf der Basis von SES, AES und QES	130
III. Pflicht: Digitalisierung formfreier Verträge	133
A. Gewillkürte Schriftform in Konzernstandards	133
B. Cloud-basierende Signatur-Workflows mit SES (und vielleicht AES)	133
C. Zusätzliche Flexibilität in der EU-Cloud	135
IV. Kür: Verträge mit Schriftformerfordernis	136
A. Besonderheiten eines QES Workflows	136

B. Vorzüge der österreichischen Handysignatur	138
C. Elektronische Signaturen und UGB/Firmenbuch	138
V. Fazit: Das Sicherste ist nicht immer das Beste	139
VI. Anhang: Häufige Fragen und Antworten	140
10. Kapitel Blockchains und Smart Contracts	142
I. Blockchains	143
A. Einführung	143
1. Begriff	143
2. Maßgebliche Prinzipien	144
3. Praktische Anwendungen	146
B. Erfassung und (zivilrechtliche) Rechtsprobleme	148
1. Rechtsbeziehungen der Teilnehmer	148
a) Offene Fragen	148
b) Kontroversen über Kontroversen	148
c) Welche Fragen sind daher konkret zu stellen?	149
2. Rechtsbeziehungen zu sonstigen „Nutzern“	150
C. Regulierung	150
II. Smart Contracts	151
A. Einführung	151
1. Begriffsbestimmung	151
2. Abwicklung on-chain – off-chain denkbar	152
B. Einige vertragsrechtliche Aspekte	152
1. Fragestellungen	152
2. Ist der Code der Vertrag?	152
a) Automatisierung als Problem?	152
b) Verständlichkeit	152
3. Wie kommt man zum Vertragsabschluss?	153
C. Problem: Finalität der Transaktion	154
D. Hemmschuh Verbraucherschutz?	155
E. Anwendbares Recht	156
11. Kapitel E-Commerce und Kartellrecht	157
I. Einleitung	158
II. Rechtliche Rahmenbedingungen	160
A. Das Kartellverbot und das Verbot des Missbrauchs einer marktbeherrschenden Stellung	160
B. Vertikale Beschränkungen	162
1. Selektive Vertriebssysteme	164
2. Preisbindung der zweiten Hand	165
3. Dualvertrieb	166
4. Doppelpreissysteme	166
5. Sonstige Wettbewerbsbeschränkungen im Online-Vertrieb	166
a) Drittplattformverbote	166
b) Verbot der Nutzung von Preisvergleichs- und Preissuchmaschinen	167
c) Brand-Bidding-Beschränkungen	167
d) Verbot der Nutzung von Online-Vermittlungsportalen	167
III. Praxis der Wettbewerbsbehörden	168
A. Europäische Entwicklungen	168
1. Sektoruntersuchung der Europäischen Kommission	168
2. Pierre Fabre: EuGH C-439/09	170
3. Coty: EuGH C-230/16	170
4. Jüngere Fallpraxis der Europäischen Kommission	171

Inhaltsverzeichnis

5. Deutsche Asics-Entscheidung	173
B. Auswahl österreichischer Fallpraxis	174
1. Händlerkonditionen bei Amazon	174
2. Fallpraxis zu vertikalen Beschränkungen im Bereich E-Commerce	176
IV. Digitale Plattformen	178
A. Digitale Plattformen als „Gatekeeper“	178
B. Bestpreisklauseln; Beschränkende Vereinbarungen durch Hotelbuchungsplattformen	179
C. Plattform-Verordnung	181
1. Rankings	182
2. Bevorzugung eigener Dienste	182
3. Aussetzung und Beendigung	182
4. Daten	182
5. Meistbegünstigung	182
V. Ausblick und weitere Reformen	183
12. Kapitel Intellectual Property im digitalen Zeitalter	185
I. Übersicht	185
II. Schwerpunkt Copyright im digitalen Umfeld	186
A. Grundlegendes	187
B. Die Info-RL	189
1. Das Vervielfältigungsrecht	189
2. Art 3 Info-RL	190
a) Recht der öffentlichen Wiedergabe	191
b) Recht der öffentlichen Zugänglichmachung	194
3. Technische Schutzmaßnahmen und Informationen	195
C. Ausblick – DSM-RL	196
1. Verantwortlichkeit von Internet-Plattformen	196
2. Urhebervertragsrecht	198
3. Sonstige Bestimmungen	199
III. Künstliche Intelligenzen	199
A. Was ist künstliche Intelligenz?	200
B. Schutz der künstlichen Intelligenz	200
1. Urheberrecht	200
2. Patentrecht	201
3. Gebrauchsmuster	202
4. Wettbewerbsrecht	202
C. Schutz von mittels KI erzeugter Inhalte	203
IV. Lizenzen im digitalen Umfeld	204
V. Open Source	205
A. Wofür steht „Open Source“?	206
1. Open-Source-Definition	206
2. Open Source in der Praxis	206
B. Open Source im österreichischen Recht	207
1. Urheberrecht	207
2. Haftung	209
13. Kapitel Arbeitsrecht im digitalen Umfeld	212
I. Vorbemerkung	213
II. Digitale Performance-Management-Systeme	213
A. Einführung von Systemen zur automationsunterstützten Datenverarbeitung nach § 96a Abs 1 Z 1 ArbVG	215
1. Allgemeines	215

2. Automationsunterstützte Personaldatenysteme	215
3. Digitale Performance-Management-Systeme als Personaldatenystem nach § 96a Abs 1 Z 1 ArbVG?	216
B. Einführung von Beurteilungssystemen von Arbeitnehmern nach § 96a Abs 1 Z 2 ArbVG	217
1. Allgemeines	217
2. Personalbeurteilungssysteme	217
3. Digitale Performance-Management-Systeme als Personalbeurteilungssystem nach § 96a Abs 1 Z 2 ArbVG?	218
C. Kontrollmaßnahmen nach § 96 Abs 1 Z 3 ArbVG	219
1. Allgemeines	219
2. Kontrollmaßnahmen und technische Systeme, die die Menschenwürde berühren	219
3. Digitale Performance-Management-Systeme als Kontrollmaßnahme nach § 96 Abs 1 Z 3 ArbVG?	220
III. Digitaler Personalakt	220
A. Allgemeines	220
B. Betriebsvereinbarungspflicht?	221
IV. Whistleblowing – neue RL	221
A. Allgemeines	221
B. Erfasste Bereiche	222
C. Meldekanäle	222
D. Redlichkeit der Hinweisgeber	222
E. Schutz vor Repressalien	222
F. Rechtsgrundlage für die Einrichtung interner Meldekanäle	223
V. Homeoffice	224
A. Allgemeines	224
B. Rahmenbedingungen von Homeoffice	224
1. Begriff „Homeoffice“	224
2. Abschluss von Einzelvereinbarungen	225
3. Abschluss einer Betriebsvereinbarung	226
4. Bereitstellung der digitalen Arbeitsmittel	226
5. Sonstige Arbeitsmittel und Aufwandsersatz	227
6. Arbeitszeit	228
7. Beendigung der Vereinbarung	228
8. Haftung des Arbeitnehmers im Homeoffice	228
9. Arbeitnehmerschutz	229
10. Unfallversicherungsschutz	229
C. Steuerliche Begünstigungen für die Arbeit im Homeoffice	230
1. Homeoffice-Pauschale	230
2. Differenzwerbungskosten	231
3. Erwerb von ergonomischem Mobiliar	231
4. Digitale Arbeitsmittel	231

Teil III
Digitalisierung im öffentlichen Recht

14. Kapitel Datenschutzrecht	233
I. Rechtliche Grundlagen	233
A. Unionsrecht	233
1. Allgemeines	233
2. DSGVO	235
B. Nationales Recht	235

II. Die DSGVO – Kapitel I bis IV	236
A. Allgemeine Bestimmungen (Kapitel I der DSGVO)	236
B. Grundsätze der Datenverarbeitung (Kapitel II der DSGVO)	238
C. Betroffenenrechte (Kapitel III der DSGVO)	242
D. Pflichten des Verantwortlichen und Auftragsverarbeiters	245
III. Die DSGVO – Kapitel V bis VIII	248
A. Datenübermittlung an Drittländer und internationale Organisationen (Kapitel V der DSGVO)	248
1. Allgemeines	248
2. BREXIT	250
3. Sonderfall USA	250
B. Aufsichtsbehörden nach der DSGVO (Kapitel VI der DSGVO)	250
C. Zusammenarbeit und Kohärenz (Kapitel VII der DSGVO)	252
D. Rechtsbehelfe, Haftung und Sanktionen (Kapitel VIII der DSGVO)	253
IV. Die innerstaatliche Umsetzung der DSGVO und der DSRL-PJ	254
15. Kapitel Telekommunikationsrecht	256
I. Einleitung	257
II. Der Europäische Kodex für die elektronische Kommunikation	259
A. Erweiterung des Adressatenkreises	260
B. Nutzerschutz	260
1. Ausweitung der Informationspflichten	261
2. Maßnahmen gegen Rufnummernmissbrauch	261
3. Kostenlose Rufnummernmitnahme nach Kündigung	262
C. Funkfrequenzverwaltung	262
D. Ausbau und die Nutzung von Netzen mit sehr hoher Kapazität	263
1. Beträchtliche Marktmacht – Ko-Investition und Verpflichtungszusagen	264
2. Geografische Erhebungen zum Netzausbau	264
E. Harmonisierung	265
F. Überblick über weitere Neuerungen	265
G. Nationale Umsetzung	267
III. Internet of Things und TK-Recht	267
A. Vorbemerkungen	268
B. Unionsrechtliche Überlegungen	269
C. IoT und Telekommunikationsrecht	270
1. Allgemeines	270
2. M2M als elektronischer Kommunikationsdienst	271
a) Signalübertragung	272
b) Entgeltlichkeit	273
c) Kein „Inhaltsdienst“	275
d) Öffentlicher und nicht-öffentlicher elektronischer Kommunikationsdienst	275
3. Roaming und IoT	275
4. Nummerierung bei IoT-Anwendungen	277
D. Zusammenfassung	280
IV. Infrastrukturausbau und Regulierung	280
A. Frequenzvergabe – Auktionsverfahren	280
1. Erste Phase des Vergabeprozesses	281
2. Zweite Phase des Vergabeprozesses	282
3. Dritte Phase des Vergabeprozesses	283
4. Zusammenfassung	284
B. Leitungsrechte im TKG 2003	285
1. Allgemeines	285
2. Verpflichtete	285

3. Berechtigte	286
4. Umfang von Leitungsrechten	286
5. Abgeltung und Richtsätze	287
6. Verhältnis zur Enteignung	289
7. Zusammenfassung	289
V. Vertragsrecht und Netzneutralität im Telekommunikationsrecht	290
A. Vertragsrecht und AGB-Kontrolle im Telekommunikationsrecht	290
1. Überblick	290
2. Einseitige Vertragsänderung	291
3. Vertragliches und gesetzliches Änderungsrecht	292
4. Indexanpassung	293
5. Vertragslaufzeiten und Kündigungsbedingungen	293
6. Internetgeschwindigkeit bei Mobilfunkverträgen	294
B. Netzneutralität	295
1. Überblick	295
2. Zero Rating und Netzneutralität	297
3. Zulässiges Verkehrsmanagement	297
4. Netzsperrungen zu Online-Inhalten	298
5. Ausblick TKG 2021	299
VI. Schlussbemerkungen	300
16. Kapitel IT-Strafrecht	301
I. IT-Strafrecht im Überblick	302
A. Begriff des IT-Strafrechts und Cybercrime	303
B. Historische Entwicklung	304
C. Materielles „Cyber-Strafrecht“ im engeren Sinn	305
1. Einleitung	305
2. Widerrechtlicher Zugriff auf ein Computersystem (§ 118 a StGB)	306
a) Objektiver Tatbestand	306
b) Subjektive Tatseite	306
c) Strafdrohung	307
3. Verletzung des Telekommunikationsgeheimnisses (§ 119 StGB)	307
a) Objektiver Tatbestand	307
b) Subjektive Tatseite	308
c) Strafdrohung	308
4. Missbräuchliches Abfangen von Daten (§ 119 a StGB)	308
a) Allgemeines	308
b) Objektiver Tatbestand	308
c) Subjektive Tatseite	309
d) Strafdrohung	309
5. Missbrauch von Tonaufnahme- oder Abhörgeräten (§ 120 StGB)	309
a) Vorbemerkung	309
b) Objektiver Tatbestand	309
c) Subjektive Tatseite	310
d) Strafdrohung	310
6. Datenbeschädigung (§ 126 a StGB)	310
a) Objektiver Tatbestand	310
b) Subjektive Tatseite	310
c) Strafdrohung	310
7. Störung der Funktionsfähigkeit eines Computersystems (§ 126 b StGB)	311
a) Objektiver Tatbestand	311
b) Subjektive Tatseite	311
c) Strafdrohung	311

8. Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c StGB) . . .	312
a) Objektiver Tatbestand	312
b) Subjektive Tatseite	312
c) Strafdrohung	312
9. Betrügerischer Datenverarbeitungsmissbrauch (§ 148a StGB)	313
a) Allgemeines	313
b) Objektiver Tatbestand	313
c) Subjektive Tatseite	313
d) Strafdrohung	313
10. Tätige Reue (§ 167 StGB)	313
11. Datenfälschung (§ 225a StGB)	314
a) Allgemeines	314
b) Objektiver Tatbestand	314
c) Subjektive Tatseite	314
d) Strafdrohung	315
D. Sonstiger Cybercrime im weiteren Sinne	315
II. Strafermittlungen und Cybercrime	319
A. Anwendung des österreichischen Strafrechts	319
1. Einleitung	319
2. Anknüpfung des StGB	319
B. „Cyber-Ermittlungen“ und Maßnahmen der StPO	320
1. Einleitung	320
2. Strafprozessordnung	320
a) Sicherstellung (§ 110 StPO)	320
aa) Anwendungsbereich	321
bb) Sonderfall „Datencloud“	322
cc) Sicherstellungsgegenstand Smartphone	322
b) Beschlagnahme (§ 115 StPO)	324
c) Durchsuchung von Orten und Gegenständen sowie von Personen (§§ 119ff StPO)	324
d) Auskunft über Stamm- und Zugangsdaten (§ 76a StPO)	325
aa) Stammdatenauskunft nach § 76a Abs 1 StPO	325
bb) Zugangsdatenauskunft gemäß § 76a Abs 2 StPO	325
e) Beschlagnahme von Briefen, Auskunft über Daten einer Nachrichtenübermittlung, Lokalisierung einer technischen Einrichtung, Anlassdatenspeicherung und Überwachung von Nachrichten (§ 135 StPO)	326
aa) Beschlagnahme von Briefen (Abs 1)	326
bb) Auskunft über Daten einer Nachrichtenübermittlung (Abs 2)	327
cc) Lokalisierung einer technischen Einrichtung (Abs 2a)	327
dd) Anlassdatenspeicherung (Abs 2b)	328
ee) Überwachung von Nachrichten (Abs 3)	328
f) Verdeckte Ermittlung (§ 131 StPO)	328
g) Scheingeschäfte (§ 132 StPO)	329
3. Sicherheitspolizeiliche Maßnahme und Ermittlungen	330
a) Vorbemerkung	330
b) Anwendungsbereich	330
c) Befugnisse nach dem SPG	330
4. Polizeilicher Staatsschutz	331
a) Einleitung und historische Entwicklung	331
b) Aufgaben nach dem PStSG	332
c) Ausgewählte Befugnisse des PStSG	333
17. Kapitel E-Government	334
I. E-Government: Was ist das? Das E-GovG	335

A. Einleitung	335
B. Das E-Government-Gesetz	336
1. Rechtliche Grundlagen	336
2. Allgemeines zum E-GovG	337
a) Vorbemerkung	337
b) Gegenstand und Ziele des Gesetzes	338
c) Recht auf elektronischen Verkehr	338
d) Für Unternehmen: Verpflichtende elektronische Zustellung	338
3. Technische Vorkehrungen des E-GovG	340
a) Die Bürgerkarte	341
b) Elektronischer Identitätsnachweis	342
aa) Die Funktion E-ID	342
bb) E-ID und Stellvertretung	342
c) Registrierung zur Nutzung der E-ID	343
d) Eindeutige Identifikation mittels Stammzahl	343
e) bPK: Das bereichsspezifische Personenkennzeichen	344
f) Zusammenfassung	344
g) Exkurs: Die App „Digitales Amt“	344
4. Verwendung des E-ID im privaten Bereich	345
5. E-ID-Verwendung mit Auslandsbezug	345
6. Elektronischer Datennachweis	345
a) Nachweis über selbstständige wirtschaftliche Tätigkeiten	346
b) Personenbezogene Daten aus Registern	346
7. Besonderheiten elektronischer Aktenführung: Die Amtssignatur	346
8. Haftungs- und Strafbestimmungen	348
C. Exkurs: E-Governance	348
1. Was ist E-Governance?	348
2. Der „Multistakeholder“-Ansatz	349
II. FinanzOnline et al: Amtsweg online	349
A. Einleitung	349
B. FinanzOnline	350
1. Vorgaben der Bundesabgabenordnung	350
a) Exkurs: Eingaben mittels Fax	351
b) Exkurs: Eingaben per E-Mail	351
2. FinanzOnline: Die Rechtsgrundlagen	352
a) FinanzOnline-Verordnung (1998)	352
b) FinanzOnline-Verordnung 2002	352
c) FinanzOnline-Verordnung 2006	353
d) FinanzOnline-Erklärungsverordnung	353
3. Die Anwendung von FinanzOnline	354
a) Allgemeines	354
b) Teilnehmer und Anmeldung	355
c) Grundlegende Funktionen von FinanzOnline	355
d) Elektronische Zustellung	356
e) Entrichtung von Abgaben	356
f) Ausschluss von Teilnehmern	357
g) Weitere Vorgaben	357
C. Sonstiges Verwaltungsverfahren	357
1. Allgemeines Verwaltungsverfahrensgesetz	357
a) Rechtliche Ausgangslage	357
b) Einbringen per E-Mail	358
c) Aktenvermerk	358
d) Erledigungen	359

2. Zustellgesetz	359
a) Vorbemerkung	359
b) Allgemeines zur elektronischen Zustellung	359
c) Elektronische Zustellmöglichkeiten	360
d) Teilnehmerverzeichnis	360
e) Anzeigemodul	361
f) Zustelldienste	361
g) Weitere Möglichkeiten ohne Zustellnachweis	363
3. Elektronischer Rechtsverkehr	363
a) Allgemeines	363
b) Funktionsweise und Nutzung des ERV	364
4. Exkurs: JustizOnline	365

Teil IV

Rechtliche Spezialfragen der Digitalisierung

18. Kapitel Rechtliche Aspekte für Start-up-Unternehmen	367
I. Definition von Start-ups und FinTechs	369
II. Rechtsform von Start-ups	369
III. Welche Genehmigungen brauchen FinTechs?	370
A. Konzessionspflichten	370
1. Konzessionspflichten nach dem BWG	370
2. Konzessionspflichten nach dem WAG 2018	371
3. Konzessionspflichten nach dem ZaDiG 2018	372
4. Konzessionspflichten nach dem E-Geld-Gesetz	372
B. Prospektpflicht und Crowd-Funding	372
C. Investitionskontrolle	373
D. Regulatory Sandbox	374
IV. Wer finanziert FinTechs oder Start-ups?	374
A. Corporate Venture Capital	375
B. Öffentliche Investoren: Public Venture Capital	375
C. Institutionelle Investoren: Venture Capital Fonds	375
D. Private Investoren	375
V. Strukturierung der Finanzierung	376
A. Einleitung	376
B. Wandeldarlehen	376
C. Kapitalerhöhung	378
1. Kapitalerhöhungsbeschluss	378
2. Übernahme der neuen Anteile	379
D. Gesellschafterzuschuss mit Anteilerwerb	380
VI. Das Vertragswerk	380
A. Vorvertragliche Vereinbarungen	380
1. Die Vertraulichkeitsvereinbarung	380
2. Letter of Intent und Memorandum of Understanding	381
3. Der Vorvertrag	382
4. Die Punktation	382
B. Der Beteiligungsvertrag	383
C. Die Gesellschaftervereinbarung	384
D. Der Gesellschaftsvertrag	385
1. Mindestinhalt	385
2. Fakultativer Inhalt	387
VII. Grundloser Abbruch von Vertragsverhandlungen	388
VIII. Zusammenfassung	389

19. Kapitel Rechtliche Gründungserfahrungen mit Start-ups	391
I. Einleitung	391
II. Vor der Gründung	392
A. Auswahl der passenden Rechtsform	392
B. Auswahl der Struktur	393
C. Auswahl der Mitgesellschafter	393
D. Patt-Situationen vermeiden	394
E. Businessplan	394
F. Gewerberecht	394
III. Gründung	394
A. Gesellschaftsvertrag	394
B. Geschäftsführung	395
C. Syndikatsvertrag	395
D. Stimmrechte & Quoren	396
E. Ausstiegszenario	396
F. Aufgriffsrechte	397
G. Tag Along – Mitverkaufsrecht	397
H. Drag Along – Mitverkaufspflicht	397
I. Kündigungsrecht	398
IV. Unternehmensführung	398
A. Non Disclosure Agreement (NDA)	398
B. Markenmeldung	399
C. Patente	400
D. Mitarbeiterbeteiligung	400
E. Allgemeine Geschäftsbedingungen (AGB)	401
V. Mitarbeiter	401
VI. Finanzierung	402
VII. Anteilsverkauf	403
A. Teilverkauf mit Optionen	403
B. Komplettverkauf	403
VIII. Persönliche Ex-post-Betrachtung	404
20. Kapitel Social Media	405
I. Rechtliche Grundlagen für Unternehmer auf Social Media	406
A. Einschlägige Rechtsnormen	406
1. ABGB	407
2. Grundrechte	408
3. Sonstige	409
B. Informations- und Offenlegungspflichten	409
1. Umfang der Offenlegungspflicht	409
2. Konsequenzen bei Verstoß	409
II. Shitstorms und negative Äußerungen	410
A. Shitstorm – Begriffsdefinition	410
B. Anspruchsgrundlagen	410
1. Zivilrechtliche Tatbestände	411
2. Wettbewerbsrechtliche Ansprüche	412
3. Medienrechtliche Ansprüche	412
4. Strafrechtliche Ansprüche	413
C. Providerhaftung	414
D. NEU: Hass-im-Netz-Gesetzespaket	415
1. KoPI-G	416
2. HiNBG	417
III. Rechte Dritter beim Aufbau einer Social-Media-Seite	418

A. Urheberrecht	419
B. Markenrecht	422
IV. Kennzeichnungspflichten bei Influencer-Marketing	423
A. Influencer-Marketing – Definition	423
B. Kennzeichnungspflicht	423
C. Art der Kennzeichnung	425
V. Bedeutung von Social-Media-Guidelines	425
A. Wozu Social-Media-Guidelines?	425
B. Inhalt von Social-Media-Guidelines	426
VI. Datenschutzrechtliche Überlegungen	427
A. Die datenschutzrechtlichen Verantwortlichkeiten	427
1. Definition des „Verantwortlichen“	427
2. Unternehmen als eigenständige Verantwortliche	428
3. Unternehmen als gemeinsame Verantwortliche	428
a) Facebook Fanpages	428
b) Social Plugins	429
B. Pflichten unter der DSGVO	429
1. Im Überblick	429
2. Informationspflichten	430
C. Die Betroffenenrechte	431
D. Datenübermittlungen in Drittländern	431
E. Nutzung von Personenbildnissen	432
1. Recht am eigenen Bild	433
2. Datenschutz	433
21. Kapitel Online-Banking	436
I. Allgemeines	437
II. Gesetzliche Grundlagen	437
III. Vorvertragliche Informationspflichten und Vertragsabschluss	438
A. FernFinG	438
1. Anwendbarkeit beim Online-Banking	438
2. Informationspflichten	438
3. Rücktrittsrecht	439
B. §§ 35 und 37 a BWG	440
1. Preisangaben auf der Internetseite	440
2. Informationen zur Einlagensicherung	440
C. ZaDiG 2018	441
1. Anforderungen an den Rahmenvertrag	441
2. Dauerhafter Datenträger, Mitteilung	441
3. Mailbox des Online-Banking	442
4. Abschluss des Rahmenvertrags	443
a) Formfreiheit	443
b) Identitätsprüfung	443
c) Sicherstellung der Rechtsverbindlichkeit	444
D. Verbraucherkreditgesetz-VKrG/Hypothekar- und Immobilienkreditgesetz-HIKrG	444
1. Vorvertragliche Information	444
2. Vertragsabschluss	445
E. Vorvertragliche Informationen und Vertragsabschluss im Wertpapiergeschäft ..	445
IV. Bankgeheimnisbindung	446
V. Erfüllung von Informationsverpflichtungen im Online-Banking	447
A. Diverse Regelungen in Materiengesetzen	447
B. Allgemein geltende Grundsätze zur Mitteilung auf dauerhaftem Datenträger/On- line-Banking-Mailbox	447

VI. Kundenaufträge, starke Kundenauthentifizierung	448
A. Allgemein	448
B. Rechtslage nach dem ZaDiG 2018	449
1. Autorisierung durch den Kunden	449
2. Bestreitung durch den Kunden	450
3. Erstattungspflicht des Zahlungsdienstleisters	450
4. Starke Kundenauthentifizierung	451
VII. Kontoinformation- und Zahlungsauslösedienstleister	452
22. Kapitel Judikatur – die drei wichtigsten Leading Cases	456
I. Einleitung	456
II. OGH 4 Ob 74/19i und EuGH C-500/19 (Puls 4 TV vs YouTube)	457
A. Sachverhalt	458
B. Innerstaatliches Verfahren	459
1. Unterinstanzliches Verfahren	459
2. Vorabentscheidungsverfahren OGH	460
C. Verfahren beim EuGH	462
1. Vorgeschichte: Der Begriff der öffentlichen Wiedergabe iSd Art 3 Info-RL	462
2. Vorabentscheidungsersuchen BGH	463
3. Keine Haftung von YouTube für Urheberrechtsverletzungen seiner Nutzer	464
III. OGH 6 Ob 195/19y und EuGH C-18/18 (Glawischnig-Piesczek vs. Facebook)	467
A. Sachverhalt	468
B. Innerstaatliches Verfahren	468
1. Unterinstanzliches Verfahren	468
2. Vorabentscheidungsverfahren OGH	469
C. Verfahren beim EuGH	471
D. Vorläufiger Zwischenstand	473
IV. Private Facebook-Gruppe doch öffentlich?	474
A. Sachverhalt	474
B. Unterinstanzliches Verfahren	475
C. Verfahren beim OGH	475
23. Kapitel Künstliche Intelligenz	478
I. Allgemein	479
A. Begriff	479
B. Europäische Initiativen	480
II. Geltendes Recht	492
A. Datenschutzrecht	492
B. Haftungsrecht	495
1. Verschuldenshaftung	495
2. Gefährdungshaftung	496
a) Produkthaftungsgesetz	496
b) EKHG	498
c) Allgemeine Gefährdungshaftung	498
C. Urheberrecht	498
1. KI-generierte Schaffung urheberrechtlich relevanter Werke („Downstream“)	498
2. Verwendung urheberrechtlich geschützter Werke („Upstream“)	502
Stichwortverzeichnis	505