

Inhaltsverzeichnis

Vorwort	V
I. Einführung	1
1. „Leitfaden“	1
2. EU-Digitalstrategie/EU-Datenstrategie	8
3. EU-Datenräume	14
4. Überblick über die behandelten Gesetze	15
II. Sicherheit in der EU	21
1. Cybersecurity Act (CA)	21
a) Zielrichtung	21
b) Inkrafttreten/Anwendbarkeit	21
c) Anwendungsbereich	22
d) Pflichten von Akteuren	22
e) Sanktionen/Geldbußen	23
f) Zuständige Aufsichtsbehörden	23
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	24
2. Cyber Solidarity Act (CSA)	27
a) Zielrichtung	27
b) Inkrafttreten/Anwendbarkeit	28
c) Anwendungsbereich	29
d) Pflichten von Akteuren	30
e) Sanktionen/Geldbußen	31
f) Zuständige Aufsichtsbehörden	31
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	32
III. (Erweiterter) KRITIS-Bereich	33
1. NIS2-Richtlinie (NIS2)	34
a) Zielrichtung	34
b) Inkrafttreten/Anwendbarkeit	35
c) Anwendungsbereich	35
d) Pflichten von Akteuren	43
EU-Mitgliedstaaten	43
Einrichtungen	44
Leitungspersonen	47
e) Sanktionen/Geldbußen	47
f) Zuständige Aufsichtsbehörden	49
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	53
1. NIS2-Umsetzungsverordnung (NIS2UmsVO)	53
2. ENISA-Leitlinien	55

- 3. NIS2-Umsetzungs- und Cybersicherheitsstärkungs-
gesetz (NIS2UmsuCG)..... 55
 - 4. ISO/IEC 27001..... 55
 - 5. BSI IT-Grundschutz..... 57
- 2. NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
(NIS2UmsuCG)..... 60
 - a) Zielrichtung..... 60
 - b) Inkrafttreten/Anwendbarkeit..... 60
 - c) Anwendungsbereich..... 61
 - d) Pflichten von Akteuren..... 64
 - 1. Risikomanagementmaßnahmen (§ 30 BSIG)..... 64
 - 2. Meldepflichten (§ 32 BSIG)..... 65
 - 3. Registrierungspflicht (§ 33 BSIG)..... 65
 - 4. Unterrichtungspflichten (§ 35 BSIG)..... 66
 - 5. Besondere Pflichten für Geschäftsleitungen..... 66
 - e) Sanktionen/Geldbußen..... 66
 - f) Zuständige Aufsichtsbehörden..... 67
 - g) Ergänzende Rechtsakte, Leitlinien, Normen & Co..... 67
- 3. CER-Richtlinie (CER)..... 68
 - a) Zielrichtung..... 68
 - b) Inkrafttreten/Anwendbarkeit..... 69
 - c) Anwendungsbereich..... 69
 - d) Pflichten von Akteuren..... 71
 - e) Sanktionen/Geldbußen..... 73
 - f) Zuständige Aufsichtsbehörden..... 73
 - g) Ergänzende Rechtsakte, Leitlinien, Normen & Co..... 73
- 4. KRITIS-Dachgesetz..... 78
 - a) Zielrichtung..... 78
 - b) Inkrafttreten/Anwendbarkeit..... 80
 - c) Anwendungsbereich..... 80
 - d) Pflichten von Akteuren..... 81
 - e) Sanktionen/Geldbußen..... 82
 - f) Zuständige Aufsichtsbehörden..... 82
 - g) Ergänzende Rechtsakte, Leitlinien, Normen & Co..... 83
- 5. IT-Sicherheitsgesetz 2.0 (IT-SiG2)..... 84
 - a) Zielrichtung..... 84
 - b) Inkrafttreten/Anwendbarkeit..... 84
 - c) Anwendungsbereich..... 85
 - d) Pflichten von Akteuren..... 86
 - e) Sanktionen/Geldbußen..... 87
 - f) Zuständige Aufsichtsbehörden..... 88
- 6. BSI-Gesetz (BSIG)..... 88

a) Zielrichtung.	88
b) Inkrafttreten/Anwendbarkeit.	89
c) Anwendungsbereich.	89
Bundesverwaltung und öffentlicher Sektor.	89
Kritische Infrastrukturen (KRITIS).	90
d) Pflichten von Akteuren.	90
Aufgaben des BSI.	90
Pflichten von KRITIS-Betreibern.	93
e) Sanktionen/Geldbußen.	94
f) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	94
IV. Datenschutz.	95
1. Datenschutzgrundverordnung (DSGVO).	99
a) Zielrichtung.	99
b) Inkrafttreten/Anwendbarkeit.	101
c) Anwendungsbereich.	102
Sachlicher Anwendungsbereich.	102
Räumlicher Anwendungsbereich.	102
d) Pflichten von Akteuren.	102
e) Sanktionen/Geldbußen.	105
f) Zuständige Aufsichtsbehörden.	105
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	106
2. Bundesdatenschutzgesetz (BDSG).	111
a) Zielrichtung.	111
b) Inkrafttreten/Anwendbarkeit.	112
c) Anwendungsbereich.	113
d) Pflichten von Akteuren.	113
e) Sanktionen/Geldbußen.	115
f) Zuständige Aufsichtsbehörden.	116
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	116
V. Verbraucherschutz.	117
1. Digitale-Inhalte-Richtlinie (DIRL).	118
a) Zielrichtung.	118
b) Inkrafttreten/Anwendbarkeit.	119
c) Anwendungsbereich.	119
d) Pflichten von Akteuren.	119
Bereitstellungspflicht und Konformitätsanforderungen.	119
Updatepflicht.	120
Rückgabe digitaler Inhalte.	120
Einschränkungen bei Kontosperrung und Inhaltslöschung. .	120
Keine „As-is“-Klauseln mehr.	120
e) Sanktionen/Geldbußen.	120

Inhaltsverzeichnis

f) Zuständige Aufsichtsbehörden	121
2. Warenkauf-Richtlinie (WKRL)	121
a) Zielrichtung	121
b) Inkrafttreten/Anwendbarkeit	122
c) Anwendungsbereich	123
d) Pflichten von Akteuren	124
Pflichten der Verkäufer	124
Pflichten der Hersteller	125
e) Sanktionen/Geldbußen	125
f) Zuständige Aufsichtsbehörden	125
3. Digital Fairness Act (DFA)	126
a) Zielrichtung	126
b) Inkrafttreten/Anwendbarkeit	127
c) Anwendungsbereich	127
d) Pflichten von Akteuren	128
4. Ökodesign-Verordnung (ÖkodesignVO)	129
a) Zielrichtung	129
b) Inkrafttreten/Anwendbarkeit	129
c) Anwendungsbereich	130
d) Pflichten von Akteuren	131
Hersteller als Hauptverantwortliche	131
Regeln für Importeure	131
Pflichten von Vertreibern und Händlern	131
Regeln für Online-Marktplätze	132
Digitaler Produktpass als zentrales Element	132
e) Sanktionen/Geldbußen	132
f) Zuständige Aufsichtsbehörden	133
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	133
VI. Produktsicherheit	135
1. Produktsicherheitsverordnung (GPSR)	135
a) Zielrichtung	135
b) Inkrafttreten/Anwendbarkeit	136
c) Anwendungsbereich	136
d) Pflichten von Akteuren	137
e) Sanktionen/Geldbußen	139
f) Zuständige Aufsichtsbehörden	139
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	140
2. Produkthaftungsrichtlinie (ProdHaftRL)	141
a) Zielrichtung	141
b) Inkrafttreten/Anwendbarkeit	142
c) Anwendungsbereich	143
d) Pflichten von Akteuren	143

e) Sanktionen/Geldbußen	145
f) Zuständige Aufsichtsbehörden	145
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	145
3. Cyber Resilience Act (CRA)	146
a) Zielrichtung.	146
b) Inkrafttreten/Anwendbarkeit.	147
c) Anwendungsbereich	147
d) Pflichten von Akteuren	150
e) Sanktionen/Geldbußen	155
f) Zuständige Aufsichtsbehörden	157
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	158
4. Maschinenverordnung (MaschinenVO)	159
a) Zielrichtung.	159
b) Inkrafttreten/Anwendbarkeit.	159
c) Anwendungsbereich	160
d) Pflichten von Akteuren	162
Hersteller.	162
Importeure.	163
Händler	163
Bevollmächtigte	163
e) Sanktionen/Geldbußen	163
f) Zuständige Aufsichtsbehörden	164
5. Funkanlagen-Richtlinie (RED)	164
a) Zielrichtung.	164
b) Inkrafttreten/Anwendbarkeit.	165
c) Anwendungsbereich	165
d) Pflichten von Akteuren	166
e) Sanktionen/Geldbußen	167
f) Zuständige Aufsichtsbehörden	167
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	167
VII. Künstliche Intelligenz	169
1. KI-Verordnung (KI-VO)	172
a) Zielrichtung.	172
Aufbau/Struktur des Gesetzes.	173
Gesetzlich verankerte Prinzipien	175
b) Inkrafttreten/Anwendbarkeit.	183
c) Anwendungsbereich	184
Bereichsausnahmen.	184
Räumlicher Anwendungsbereich	185
Sachlicher Anwendungsbereich	186
Persönlicher Anwendungsbereich.	189
d) Pflichten von Akteuren	192

Einteilung in Risikoklassen.	192
Anforderungen an Hochrisiko-KI-System; Anbieter- & Betreiber-Pflichten	205
Anforderungen an KI-Modelle mit allgemeinem Verwendungszweck.	209
Transparenzpflichten.	212
KI-Kompetenz.	216
e) Sanktionen/Geldbußen	223
f) Zuständige Aufsichtsbehörden	225
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	226
ISO/IEC 42001 (KI-Managementsystem)	226
ISO 31000 (Risikomanagement).	226
ISO/IEC 27001 (Informationssicherheitsmanagement)	226
IT-Einsatz-Gesetz (ITEG).	226
BSI AIC4.	229
BRAK-Leitfaden zum KI-Einsatz.	230
Leitlinien für KI-Einsatz in der Bundesverwaltung	230
Initiativen	231
GPAI Code of Practice	236
h) Checkliste KI-VO	237
2. KI-Haftungsrichtlinie (KI-HaftRL).	239
a) Zielrichtung.	239
b) Inkrafttreten/Anwendbarkeit.	241
c) Anwendungsbereich	241
d) Pflichten	241
VIII. Daten(wirtschafts)recht	243
1. Data Act (DA)	243
a) Zielrichtung.	243
b) Inkrafttreten/Anwendbarkeit.	244
c) Anwendungsbereich	244
d) Pflichten von Akteuren	245
e) Sanktionen/Geldbußen	246
f) Zuständige Aufsichtsbehörden	247
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	248
2. Data Governance Act (DGA)	249
a) Zielrichtung.	249
b) Inkrafttreten/Anwendbarkeit.	250
c) Anwendungsbereich	250
d) Pflichten von Akteuren	251
e) Sanktionen/Geldbußen	251
f) Zuständige Aufsichtsbehörden	253
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	254

3. Geschäftsgeheimnisgesetz (GeschGehG)	254
a) Zielrichtung.	254
b) Inkrafttreten/Anwendbarkeit.	255
c) Anwendungsbereich	255
d) Pflichten von Akteuren	256
e) Sanktionen/Geldbußen	257
f) Zuständige Aufsichtsbehörden	258
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	258
IX. Finanzsektor	259
1. Digital Operational Resilience Act (DORA).	259
a) Zielrichtung.	259
b) Inkrafttreten/Anwendbarkeit.	260
c) Anwendungsbereich	260
Finanzunternehmen:	261
IKT-Dienstleister.	262
d) Pflichten von Akteuren	263
e) Sanktionen/Geldbußen	265
f) Zuständige Aufsichtsbehörden	265
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	266
Ergänzende EU-Regelungen.	266
Deutsche Regelungen	268
MaRisk	269
2. Framework for Financial Data Access (FiDA)	270
a) Zielrichtung.	270
b) Inkrafttreten/Anwendbarkeit.	270
c) Anwendungsbereich	271
d) Pflichten von Akteuren	272
e) Sanktionen/Geldbußen	273
f) Zuständige Aufsichtsbehörden	273
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	274
3. Markets in Crypto-Assets Regulation (MiCAR).	274
a) Zielrichtung.	274
b) Inkrafttreten/Anwendbarkeit.	275
c) Anwendungsbereich	275
Erfasste Kryptowerte	275
d) Pflichten von Akteuren	276
e) Sanktionen/Geldbußen	277
f) Zuständige Aufsichtsbehörden	277
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	278
Europäische Standards	278
Deutsche Regelungen	278
4. Finanzmarktdigitalisierungsgesetz (FinmadiG)	280

a) Zielrichtung.....	280
b) Inkrafttreten/Anwendbarkeit.....	280
c) Anwendungsbereich	280
d) Pflichten von Akteuren	281
e) Zuständige Aufsichtsbehörden	282
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	282
X. Gesundheitssektor.....	283
1. European Health Data Space (EHDS).....	283
a) Zielrichtung.....	283
b) Inkrafttreten/Anwendbarkeit.....	283
c) Anwendungsbereich	284
Primärnutzung.....	284
Sekundärnutzung.....	284
d) Pflichten von Akteuren	285
e) Sanktionen/Geldbußen	286
f) Zuständige Aufsichtsbehörden	286
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	287
2. Medizinprodukteverordnung (MDR)	288
a) Zielrichtung.....	288
b) Inkrafttreten/Anwendbarkeit.....	289
c) Anwendungsbereich	289
d) Pflichten von Akteuren	290
e) Sanktionen/Geldbußen	290
f) Zuständige Aufsichtsbehörden	291
3. Patientendatenschutzgesetz (PDSG)	291
a) Zielrichtung.....	291
b) Inkrafttreten/Anwendbarkeit.....	292
c) Anwendungsbereich	292
d) Pflichten von Akteuren	293
e) Sanktionen/Geldbußen	293
f) Zuständige Aufsichtsbehörden	294
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	294
4. Gesundheitsdatennutzungsgesetz (GDNG).....	295
a) Zielrichtung.....	295
b) Inkrafttreten/Anwendbarkeit.....	295
c) Anwendungsbereich	295
d) Pflichten von Akteuren	296
e) Sanktionen/Geldbußen	296
f) Zuständige Aufsichtsbehörden	297
g) Ergänzende Rechtsakte, Leitlinien, Normen & Co.	297
5. Digitale-Versorgung-Gesetz (DVG)	298
a) Zielrichtung.....	298

- b) Inkrafttreten/Anwendbarkeit. 298
- c) Anwendungsbereich 299
- d) Pflichten von Akteuren 300
- e) Sanktionen/Geldbußen 300
- f) Zuständige Aufsichtsbehörden 300
- g) Ergänzende Rechtsakte, Leitlinien, Normen & Co. 301
- XI. Plattformregulierung 303**
 - 1. Platform-to-Business-Verordnung (P2B-VO) 303
 - a) Zielrichtung. 303
 - b) Inkrafttreten/Anwendbarkeit. 303
 - c) Anwendungsbereich 303
 - d) Pflichten von Akteuren 304
 - e) Sanktionen/Geldbußen 305
 - f) Zuständige Aufsichtsbehörden 306
 - g) Ergänzende Rechtsakte, Leitlinien, Normen & Co. 306
 - 2. Digital Services Act (DSA) 306
 - a) Zielrichtung. 306
 - b) Inkrafttreten/Anwendbarkeit. 307
 - c) Anwendungsbereich 307
 - d) Pflichten von Akteuren 310
 - e) Sanktionen/Geldbußen 311
 - f) Zuständige Aufsichtsbehörden 312
 - g) Ergänzende Rechtsakte, Leitlinien, Normen & Co. 313
 - 3. Digital Markets Act (DMA) 313
 - a) Zielrichtung. 313
 - b) Inkrafttreten/Anwendbarkeit. 314
 - c) Anwendungsbereich 314
 - d) Pflichten von Akteuren 316
 - e) Sanktionen/Geldbußen 317
 - f) Zuständige Aufsichtsbehörden 317
 - g) Ergänzende Rechtsakte, Leitlinien, Normen & Co. 317
 - 4. Digital Networks Act (DNA) 318
 - a) Zielrichtung. 318
 - b) Inkrafttreten/Anwendbarkeit. 319
 - c) Anwendungsbereich 320
 - d) Pflichten von Akteuren 320
 - e) Sanktionen/Geldbußen 320
 - f) Zuständige Aufsichtsbehörden 321