

Vorwort	13
1 Einleitung	15
1.1 Cloud Computing und Datenschutz im Spannungsfeld	16
1.2 Cloud Computing: flexible Nutzung von IT	17
1.3 Datenschutz, Datensicherheit und Compliance	19
2 Cloud Computing: Einführung, Basics und wichtigste Begriffe	21
2.1 Cumulus oder Stratus: Was ist Cloud Computing?	22
2.2 Begriffsklärung und begriffliche Entwicklung	23
2.2.1 Die »NIST Definition of Cloud Computing«	23
2.2.2 Definition des BSI	24
2.2.3 Wie Cloud Computing in diesem Buch verstanden wird ..	24
2.3 Technische Grundlagen »in a Nutshell«	25
2.3.1 Technische Rahmenbedingungen	25
2.3.2 Basistechnologien	26
2.4 Cloud-Service-Modelle	31
2.4.1 Infrastructure as a Service (IaaS)	31
2.4.2 Platform as a Service (PaaS)	35
2.4.3 Software as a Service (SaaS)	36
2.5 Cloud-Bereitstellungsformen	39
2.5.1 Public Cloud	39
2.5.2 Private Cloud	41
2.5.3 Hybrid Cloud	43
2.5.4 Multi Cloud	45
2.5.5 Community Cloud	46
2.6 Begriffsvielfalt und weitere Unterscheidungen	47
2.7 AWS, Google und Microsoft – Kurzporträts und Standorte der jeweiligen Cloud-Infrastrukturen	48
2.7.1 Amazon Web Services (AWS)	48

2.7.2	Google Cloud Platform (GCP)	51
2.7.3	Microsoft Azure und Microsoft 365	54
3	Datenschutz nach der DSGVO: Einführung und wichtigste Basics für die Cloud-Computing-Praxis	59
3.1	Datenschutz und informationelle Selbstbestimmung.	59
3.2	Datenschutzreform.	62
3.3	Cloud Computing und die Datenschutzreform	63
3.4	Warum ist der Datenschutz im Cloud Computing und in einer digitalen Welt so wichtig?	64
3.5	DSGVO-Basics im Cloud Computing: zentrale Begriffe und Grundprinzipien des »Daten-Schutz-Rechts«.	67
3.5.1	»Daten« – Verarbeitung personenbezogener Daten	67
3.5.2	»Schutz« – Verbot mit Erlaubnisvorbehalt	68
3.5.3	»Recht« – Rechtmäßigkeit der Datenverarbeitung	69
3.5.4	Die wichtigsten Akteure im Datenschutz	72
3.5.5	Die Landkarte des Datenschutzes.	83
3.5.6	Aufbau der DSGVO	85
4	Wann ist die DSGVO im Cloud Computing überhaupt anzuwenden?	87
4.1	Sachlicher Anwendungsbereich: Werden personenbezogene Daten verarbeitet?	88
4.1.1	Personenbezogene Daten	88
4.1.2	Verarbeitung	93
4.1.3	Ganz oder teilweise automatisierte Verarbeitung.	94
4.1.4	Keine Ausnahme (z.B. für private Zwecke)	95
4.2	Räumlicher Anwendungsbereich: Wo und durch wen werden die Daten verarbeitet?	97
4.2.1	Verarbeitung durch eine Niederlassung in der EU (Niederlassungsprinzip)	98
4.2.2	Verarbeitung durch eine Niederlassung außerhalb der EU (Marktortprinzip)	101
4.3	Andere Rechtsgebiete	105
4.4	FAQs.	105
4.5	Checkliste zum Anwendungsbereich der DSGVO	106
5	Wann ist die Datenverarbeitung erlaubt? – Zulässigkeit (1. Stufe): Erlaubnistatbestände als Rechtsgrundlage	109
5.1	Datenverarbeitung auf Basis einer Einwilligung (Art. 6 Abs. 1 lit. a DSGVO).	112
5.2	Datenverarbeitung zur Erfüllung eines Vertrags (Art. 6 Abs. 1 lit. b DSGVO).	115

5.3	Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DSGVO)	115
5.4	Datenverarbeitung zum Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 lit. d DSGVO)	116
5.5	Datenverarbeitung zur Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe und zur Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 lit. e DSGVO)	116
5.6	Datenverarbeitung zur Wahrung berechtigter Interessen (Art. 6 Abs. 1 lit. f DSGVO)	117
5.7	Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO; »besonders sensible Daten«)	119
5.8	Bereichsspezifischer Datenschutz	120
5.9	FAQs	121
5.10	Checkliste	122
6	Auftragsverarbeitung	123
6.1	Hohe Praxisrelevanz im Cloud Computing	123
6.2	Definition der Auftragsverarbeitung und kennzeichnendes Privileg	125
6.3	Verarbeitung »im Auftrag« – Beispiele und Erscheinungsformen der Auftragsverarbeitung in der Praxis	127
6.3.1	Typische Beispiele für eine Auftragsverarbeitung	128
6.3.2	Keine Auftragsverarbeitung	130
6.3.3	Colocation als besondere Fallgestaltung im Rechenzentrumsumfeld	131
6.4	Beteiligte der Auftragsverarbeitung	132
6.5	Voraussetzungen der Auftragsverarbeitung	134
6.5.1	Sorgfältige Auswahl	134
6.5.2	Abschluss eines AV-Vertrags	136
6.5.3	Praxisprobleme bei Standardverträgen	139
6.6	Einsatz von Unterauftragsverarbeitern (den sogenannten Subunternehmern)	139
6.6.1	Genehmigung der Subunternehmer durch den Verantwortlichen	140
6.6.2	Weiterreichung der Datenschutzpflichten an den Subunternehmer	143
6.7	Auftragsverarbeitung im Ausland	144
6.7.1	Auftragsverarbeitung innerhalb von EU und EWR	145
6.7.2	Internationale Auftragsverarbeitung in Drittländern außerhalb von EU und EWR	145
6.8	Besonderheiten in regulierten Märkten	146
6.9	FAQs	146
6.10	Checkliste: Auftragsverarbeitung/AV-Vertrag	151

7	Gemeinsame Verantwortlichkeit (Joint Control)	153
7.1	Gemeinsame Verantwortlichkeit zwischen den an der Datenverarbeitung Beteiligten	154
7.2	Gemeinsame Verantwortlichkeit am Beispiel von Microsoft 365 und Google Analytics	155
7.3	FAQs	156
7.4	Checkliste	157
8	Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten	159
8.1	Rechtmäßigkeit	159
8.2	Verarbeitung nach Treu und Glauben	160
8.3	Transparenz	160
8.4	Zweckbindung	161
8.5	Datenminimierung	162
8.6	Richtigkeit	162
8.7	Speicherbegrenzung	162
8.8	Integrität und Vertraulichkeit	162
8.9	Rechenschaftspflicht	163
8.10	FAQs	164
8.11	Checkliste	164
9	Verarbeitungsverzeichnis	167
9.1	Pflicht zur Verzeichniserstellung	168
9.2	Verarbeitungstätigkeiten	169
9.3	Führung des Verarbeitungsverzeichnisses	171
9.3.1	Verarbeitungsverzeichnis des Verantwortlichen	171
9.3.2	Verarbeitungsverzeichnis der gemeinsam Verantwortlichen (Joint Controller)	176
9.3.3	Verarbeitungsverzeichnisse des Auftragsverarbeiters	177
9.4	FAQs	178
9.5	Checkliste	178
10	Datensicherheit	181
10.1	Klassische Schutzziele der Datensicherheit	181
10.2	Rechtsgrundlagen der Datensicherheit	183
10.2.1	Datensicherheit in der DSGVO	183
10.2.2	Datensicherheit außerhalb der DSGVO	185
10.3	Typische Gefährdungslage im Cloud Computing und Leitfaden für Datensicherheitsaspekte	187
10.4	Implementierung technischer und organisatorischer Maßnahmen in der IT-Sicherheitsarchitektur	189

10.4.1	Infrastruktur- und Rechenzentrumsebene (Gelände und Gebäude)	190
10.4.2	IT-System- und -Virtualisierungsebene	191
10.4.3	Netzwerkebene	191
10.4.4	Software-/Anwendungsebene	192
10.4.5	Ebenenübergreifende Aspekte	193
10.4.6	Weitere Vertiefung	193
10.5	Cloud-Zertifizierungen	194
10.5.1	BSI-C5-Kriterienkatalog	194
10.5.2	ISO/IEC 27001 (einschließlich ISO/IEC 27017 und 27018)	195
10.5.3	ISO 9001	196
10.5.4	BSI-IT-Grundschutz und BSI-Standards	196
10.5.5	Cloud Security Alliance	197
10.5.6	EuroCloud Star Audit	197
10.5.7	Trusted Cloud	198
10.5.8	Datenschutz Zertifizierungen nach der DSGVO	198
10.5.9	Andere Zertifizierungsverfahren	198
10.6	Notfallmanagement: Vorbereitung auf den Ernstfall	199
10.7	FAQs	199
10.8	Checkliste für einen IT-Sicherheitsvorfall	200
11	Datenschutz-Folgenabschätzung	201
11.1	Wann ist eine DSFA verpflichtend durchzuführen?	201
11.2	Wie ist eine DSFA durchzuführen, und was sind deren Inhalte?	203
11.3	Praxisbeispiel: Microsoft 365	204
11.4	FAQs	206
11.5	Checkliste	207
12	Wann dürfen Daten in Länder außerhalb der EU übermittelt werden? – Zulässigkeit (2. Stufe): Internationale Datentransfers	209
12.1	Übermittlung in Drittländer	211
12.1.1	Übermittlung	211
12.1.2	Drittland	212
12.1.3	Internationale Datentransfers im Cloud Computing.	214
12.2	Voraussetzungen für internationale Datentransfers in ein Drittland	215
12.3	Das angemessene Datenschutzniveau	216
12.4	Angemessenheitsbeschlüsse der EU-Kommission.	217
12.5	Sonderregelungen für transatlantische Datentransfers in die USA	219

12.5.1	Safe Harbor und Schrems-I-Urteil	221
12.5.2	EU-U.S. Privacy Shield, Schrems-II-Urteil und seine Folgen	222
12.5.3	Trans-Atlantic Data Privacy and Security Framework	224
12.6	Datenübermittlungen auf Grundlage geeigneter Garantien	224
12.6.1	Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules)	225
12.6.2	Standardvertragsklauseln (SCC)	226
12.6.3	Weitere geeignete Garantien	231
12.6.4	Ausnahmen nach Art. 49 DSGVO	231
12.7	FAQs	232
12.8	Checkliste	234
13	Datenzugriff durch Behörden nach dem Recht der USA	235
13.1	Nachrichtendienstliche Überwachung	236
13.2	Herausgabe von Daten als Beweismittel im Rahmen strafrechtlicher Ermittlungen: der CLOUD Act	239
13.2.1	Der CLOUD Act im Überblick	240
13.2.2	Microsoft Corp. v. United States: ein Rechtsstreit über die Herausgabe von Daten aus Irland als Anlass für den CLOUD Act	241
13.2.3	Rechtskonflikt mit der DSGVO	243
13.3	Typische Praxiskonstellationen und Handlungsempfehlungen für Unternehmen in der EU	245
13.3.1	Datenverarbeitung bei Cloud-Anbietern in der EU mit Sitz in den USA bzw. mit US-Muttergesellschaft	246
13.3.2	Datenverarbeitung bei Cloud-Anbietern in der EU mit US-Tochtergesellschaft	246
13.3.3	Handlungsempfehlungen	247
13.4	FAQs	248
13.5	Checklisten	250
13.5.1	Wie sicher sind meine Daten vor dem CLOUD Act?	250
13.5.2	Worauf habe ich zu achten, wenn ich eine datenschutzfreundliche Lösung in der EU umsetzen möchte?	251
13.5.3	Ich möchte Leistungen eines US-Hyperscalers nutzen. Wie begegne ich einem bestehenden behördlichen Zugriffsrisiko nach dem CLOUD Act oder einem anderen US-Gesetz?	251

14 Rechte der Betroffenen	253
14.1 Recht auf Information	254
14.2 Recht auf Auskunft	256
14.2.1 Was ist das Auskunftsrecht?	256
14.2.2 Form und Frist der Auskunftserteilung	257
15 Aufsichtsbehörden	259
15.1 Datenschutzaufsicht in Deutschland	260
15.2 Aufsichtsbehörden in anderen EU-Mitgliedstaaten	262
15.3 Europäische Ebene	263
16 Datenschutzbeauftragter	265
16.1 Pflicht zur Bestellung	266
16.2 Interner oder externer Datenschutzbeauftragter?	268
16.3 Datenschutzkoordinator	268
16.4 FAQs	269
16.5 Checkliste zur Bestellung eines Datenschutzbeauftragten	270
17 Umgang mit Datenschutzverletzungen	271
17.1 Dokumentations-, Melde- und Benachrichtigungspflichten im Fall einer Datenschutzverletzung	271
17.2 Notfallmanagement: Vorbereitung auf den Ernstfall und Erstellung von Notfallplänen	277
17.3 FAQs	279
17.4 Checkliste bei einer Datenschutzverletzung	279
18 Bußgelder, Sanktionen und Haftung: Welche Strafen drohen bei einem Verstoß gegen die DSGVO?	281
18.1 Bußgelder	282
18.2 Sanktionen	283
18.3 Schadensersatz und Haftung	283
19 Besonderheiten regulierter Märkte	285
19.1 Cloud Computing in der öffentlichen Verwaltung	285
19.2 Berufsgeheimnisträger (wie Rechtsanwälte, Steuerberater, Ärzte)	290
19.3 Finanzsektor (Kredit- und Finanzdienstleister, Zahlungs- institute)	294
19.4 Versicherungen	296

20 Handlungsempfehlungen für ein datenschutzkonformes Cloud Computing (im Lifecycle einer Cloud-Nutzung) 299

20.1 Marktanalyse 299

20.2 Auswahlentscheidung..... 300

20.2.1 Kommerzielle und technische Aspekte..... 300

20.2.2 Datenschutz 301

20.2.3 Weitere Aspekte im Rahmen der Auswahlentscheidung..... 305

20.3 Vertragsabschluss mit dem Cloud-Anbieter..... 305

20.4 Vertragsabschluss mit einem Reseller..... 306

20.5 Betriebsphase – was ist während der Cloud-Nutzung zu beachten? 307

20.6 Ende der Cloud-Nutzung (Exit bzw. Migration) 308

21 Bekannte Cloud-Anbieter im Check – worauf ist zu achten? 309

21.1 Amazon Web Services (AWS) 309

21.1.1 AWS-Vertragsbedingungen 309

21.1.2 Datenschutz 311

21.2 Google Cloud Platform (GCP) 315

21.2.1 Google-Vertragsbedingungen..... 315

21.2.2 Datenschutz 317

21.3 Microsoft 321

21.3.1 Microsoft-Vertragsbedingungen..... 321

21.3.2 Datenschutz 323

Anhang A Glossar..... 325

Anhang B Literaturverzeichnis 335

Index..... 337