

Inhaltsübersicht

Vorwort	V
Inhaltsverzeichnis	XIII
Bearbeitungsverzeichnis	XXXIX
Abkürzungsverzeichnis	XLIII
Literaturverzeichnis	LV

Teil A. Einführung und rechtliche Grundlagen

Kapitel 1. Einführung	1
Kapitel 2. Recht der elektronischen Kommunikation (ePrivacy)	7
A. Europäisches Recht	7
B. Nationales Recht (TDDDG)	10
Kapitel 3. Datenschutz	15
A. Datenschutz-Grundverordnung (DS-GVO)	16
B. Bundesdatenschutzgesetz (BDSG)	32
Kapitel 4. Sonstige relevante Regelungsbereiche mit Bezug zum Datenschutz	37
A. Digitale-Inhalte-Richtlinie und nationale Umsetzung in §§ 327 ff. BGB	39
B. Gesetz gegen den unlauteren Wettbewerb (UWG)	52
C. Überblick über EU-Datenakte	59

Teil B. Websites und Apps

Kapitel 5. Funktionsweise und technische Erläuterungen	69
A. Einführung	69
B. Allgemeines zur Funktionsweise des Internets	70
C. Einbindung externer Dienste	93
D. Apps	94
Kapitel 6. Zugriff und Speicherung von Informationen auf Endeinrichtungen	97
A. Allgemeines	98
B. Tracking	105
C. Ausblick	111
Kapitel 7. Datenkategorien	115
A. Einleitung: Datenkategorien im Datenschutzrecht	115
B. Personenbezogene Daten	116
C. Besondere Arten personenbezogener Daten nach Art. 9 DS-GVO	122
D. Nicht personenbezogene Daten	123
Kapitel 8. Datenschutzrechtliche Rolle der Beteiligten	127
A. Einführung	128
B. Das Rollenkonzept der DS-GVO im Einzelnen	129
C. Das Rollenkonzept des § 25 TDDDG	160
Kapitel 9. Erlaubnistatbestände der Datenverarbeitungen	163
A. Gesetzliche Erlaubnisse nach TDDDG	168
B. Gesetzliche Erlaubnisse nach DS-GVO	191

VII

Inhaltsübersicht

C. Einwilligungsbasierte Datenverarbeitung	208
Kapitel 10. Rechtfertigung einzelner Verarbeitungszwecke	259
A. Einleitung	259
B. Bereitstellung und Durchführung des Dienstes	260
C. Abrechnung	263
D. Statistische Analyse	265
E. IT-Sicherheit	268
F. Update- und Patchmanagement	271
G. Werbung und Werbefinanzierung mit Reichweitenmessung	272
H. Produktverbesserung/Produktentwicklung	275
Kapitel 11. Veröffentlichungen und Entscheidungen von Aufsichtsbehörden, Gremien und Gerichten	277
A. Veröffentlichungen der Aufsichtsbehörden und Gremien	278
B. Behördliche Entscheidungen	292
C. Gerichtsentscheidungen	298
Kapitel 12. Einbindung von Fotografien	301
A. Fotografien und personenbezogene Daten	302
B. Fotos und Datenverarbeitung im Internet	303
C. Anwendungsbereich der DS-GVO und Fotos im Internet	304
D. Rechtsgrundlage der Verarbeitung von fotobezogenen Daten	304
E. Pflichten im Zusammenhang mit der Fotodatenverarbeitung	311
Kapitel 13. Drittlandtransfer	315
A. Vorliegen eines Drittlandtransfers	316
B. Zwei-Stufen-Prüfung	317
C. Nicht zulässige Übermittlungen	318
D. Angemessenheitsbeschluss der Kommission	319
E. Geeignete Garantien	320
F. Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO)	328
Kapitel 14. Datensicherheit	333
A. Datenschutzrechtliche Grundlagen	333
B. Risikoermittlung, -analyse, -beurteilung und -behandlung sowie Sicherheit der Verarbeitung durch technische und organisatorische Maßnahmen	337
C. Privacy by Design und Privacy by Default	348
D. Genehmigte Verhaltensregeln und Zertifizierungen	349
E. Anerkannte Standards	349
Kapitel 15. Transparenz und Informationspflichten	353
A. Regelung der Transparenz in der DS-GVO	355
B. Inhalte der Informationspflichten	358
C. Zeitpunkt der Bereitstellung von Informationen	365
D. Informationspflichten bei nachträglichen Änderungen	366
E. Ausnahmen von den Informationspflichten	367
F. Art und Form der Informationsvermittlung	370
Kapitel 16. Initiativrechte der betroffenen Personen	379
A. Überblick	380
B. Modalitäten	382
C. Die Rechte im Einzelnen	390

D. Rechtsdurchsetzung	400
E. Haftung	401
Kapitel 17. Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen	403
A. Einleitung	405
B. Allgemeines	413
C. Art. 33 DS-GVO: Meldepflicht bei der zuständigen Aufsichtsbehörde	421
D. Art. 34 DS-GVO: Benachrichtigung der von einer Datenschutzverletzung betroffenen Person	428
E. Empfehlungen für die Praxis	433
Kapitel 18. Rechenschaftspflicht („Accountability“)	439
A. Sinn und Zweck der Rechenschaftspflicht	439
B. Konkretisierung der Rechenschaftspflicht	440
C. Umsetzung der Rechenschaftspflicht bei Internetangeboten	441
D. Bedeutung der Rechenschaftspflicht bei behördlichen Maßnahmen ...	442
E. Umfang und praktische Umsetzung der Rechenschaftspflicht/Einzelbereiche	449
Teil C. Spezifische Anwendungsszenarien	
Kapitel 19. Messenger	457
A. Technischer und netzökonomischer Hintergrund	458
B. Rechtlicher Rahmen	460
C. Elektronische Kommunikationsdienste und maßgebliche Bestimmungen	461
D. Einzelfragen bestimmter Dienste in spezifischen Anwendungskontexten	472
E. Vorschlag für eine Verordnung zur Festlegung von Vorschriften für die Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern („Chatkontrolle“)	474
Kapitel 20. Einsatz von Social Media im Unternehmen	477
A. Beschäftigtendatenschutz	480
B. Kunden-/Interessentendatenschutz	497
C. Spezifische Anforderungen einzelner sozialer Netzwerke	514
Kapitel 21. Datenbasierte Geschäftsmodelle im Online-Marketing	519
A. Digitale Geschäftsmodelle	522
B. Datenschutzrechtliche Verantwortlichkeit	536
C. Zulässigkeit von Verarbeitungen nach TDDDG und DS-GVO	537
D. Profiling und automatisierte Entscheidungen, Art. 22 DS-GVO	542
E. Wettbewerbsrechtliche Implikationen	544
F. Gestaltung von Einwilligungs-Bannern	549
G. Verfahren der belgischen Aufsichtsbehörde zum TCF 2.0	568
H. Werblocker	572
I. Blocker von Consent Management Plattformen	575
J. Zusammenfassung und Ausblick	579
Kapitel 22. Recht des E-Mail-Marketings	587
A. Systematik und Zusammenspiel mit der DS-GVO	588
B. Rechtsrahmen des E-Mail-Marketings	591
C. Erfolgskontrolle und Personalisierung	610
D. Widerruf und Widerspruch, Verwirkung von Erlaubnistatbeständen	614

Inhaltsübersicht

E. Abmahnungen, Ansprüche von Geschädigten und Sanktionsrisiken ...	617
Kapitel 23. Onlineshops	621
A. Einleitung	622
B. Anwendbares Recht	622
C. Datenschutzrechtliche Verantwortlichkeit	622
D. Bestellung mit und ohne Kundenkonto	625
E. Datenverarbeitungen im Bestellprozess	627
F. Einbindung von Dienstleistern und externen Partnern	631
G. Behördliche Auskunftsverlangen	634
H. Kundenservice	634
I. Maßnahmen des Direktmarketings	635
J. Informationspflichten	637
K. Technisch-organisatorische Maßnahmen	638
Kapitel 24. Computerspiele	641
A. Verarbeitungsprozesse und Rechtsgrundlagen	641
B. Datenschutzrechtliche Rolle der Beteiligten	646
Kapitel 25. Videokonferenzen – Einsatz im Beschäftigungsverhältnis	649
A. Abgrenzung TelKo – ViKo	650
B. Rechtliche Rahmenbedingungen	651
Kapitel 26. Datenschutz im Internet of Things	665
A. Einführung	665
B. Begriff des IoT und technische Grundlagen	666
C. Anwendbares Datenschutzrecht im IoT	668
D. IoT-Daten im Lichte der datenschutzrechtlichen Regelungen	669
E. Allgemeine Datenschutzprinzipien für vernetzte Endgeräte	675
F. Fazit und Ausblick	676
Kapitel 27. Connected Cars	679
A. Datensammlung in Fahrzeugen	680
B. Anwendbare Regelungen	681
C. Rechtfertigung	684
Kapitel 28. Künstliche Intelligenz	691
A. Einführung	692
B. Begriff der künstlichen Intelligenz	693
C. KI-spezifische Regulierung in Deutschland und Europa	695
D. Datenschutzrechtliche Regulierung	696
E. Bußgelder und Haftung	707
Kapitel 29. Rechtskonformer Einsatz von KI-Sprachsystemen im Unternehmen	709
A. Einführung	710
B. Datenschutzrecht	711
C. Weitere Rechtsfragen	720
D. Ausblick: KI-Verordnung	724
E. Zusammenfassung der Ergebnisse und Fazit	726
Kapitel 30. Digitaler Nachlass	729
A. Der digitale Nachlass und postmortaler Datenschutz	730
B. Vererbbarkeit von Accountverhältnissen nach den §§ 1922ff. BGB ...	731

C. Die Anforderungen der DS-GVO und der Übergang digitaler Rechte im Todesfall	738
D. Empfehlungen für den Vorsorge- und Erbfall	740
Kapitel 31. Internetdaten und Sicherheitsbehörden	749
A. Einführung	750
B. Datenerhebung beim Anbieter	754
C. Datenerhebung während des Übertragungsvorgangs	769
D. Datenerhebung bei den Beteiligten der Kommunikation	771
E. Weitere Formen der Datenerhebung	774
F. Kernbereichsschutz	775
G. Informations-, Auskunfts- und Benachrichtigungspflichten	776
H. Rechtsschutzmöglichkeiten	776
I. Zusammenfassung, Kritik und Ausblick	778
 Teil D. Risiken bei Datenschutzverstößen	
Kapitel 32. Unterlassungsansprüche	781
A. Einführung	783
B. Überblick über Unterlassungsansprüche im datenschutzrechtlichen Rechtsschutzsystem	783
C. Individualklagen auf Unterlassung	791
D. Kollektivklagen auf Unterlassung	799
E. Praxishinweise	807
F. Musterformulierung: Klage auf Unterlassung der Nutzung von Cookies	812
G. Ausblick	814
Kapitel 33. Schadensersatz	817
A. Allgemeines	818
B. Schadensersatz nach Art. 82 DS-GVO	818
Kapitel 34. Aufsichtliches Verfahren	833
A. Zuständigkeit	834
B. Verfahren	836
C. Form	838
D. Aufgaben und Befugnisse	838
E. Verteidigungsstrategien und Handlungsempfehlungen	839
Kapitel 35. Bußgeldverfahren	843
A. Verhältnis zum aufsichtsbehördlichen Verwaltungsverfahren	844
B. Verfahren	845
C. Bußgeldadressat	847
D. Materieller Bußgeldtatbestand	850
E. Bußgeldentscheidung	853
F. Behördliche Öffentlichkeitsarbeit	860
G. Rechtsschutz	860
H. Rechtskräftiges Bußgeld	861
 Stichwortverzeichnis	 863

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Bearbeitungsverzeichnis	XXXIX
Abkürzungsverzeichnis	XLIII
Literaturverzeichnis	LV

Teil A. Einführung und rechtliche Grundlagen

Kapitel 1. Einführung	1
Kapitel 2. Recht der elektronischen Kommunikation (ePrivacy)	7
A. Europäisches Recht	7
I. ePrivacy-RL	8
II. Keine ePrivacy-Verordnung	9
III. Verhältnis von ePrivacy-RL und DS-GVO	9
B. Nationales Recht (TDDDG)	10
I. Anwendungsbereich und Regelungszweck des TDDDG	10
II. Verhältnis zu anderen Rechtsakten	11
Kapitel 3. Datenschutz	15
A. Datenschutz-Grundverordnung (DS-GVO)	16
I. Sachlicher Anwendungsbereich	16
1. Allgemeines	16
2. Personenbezogene Daten	17
3. Haushaltsausnahme	24
II. Räumlicher Anwendungsbereich	28
1. Niederlassungsprinzip (Art. 3 Abs. 1 DS-GVO)	28
2. Marktortprinzip (Art. 3 Abs. 2 DS-GVO)	30
B. Bundesdatenschutzgesetz (BDSG)	32
I. Zielsetzung des BDSG	32
II. Anwendungsbereich des BDSG und Verhältnis zur DS-GVO	33
III. Praxisrelevante Regelungskomplexe im BDSG	34
Kapitel 4. Sonstige relevante Regelungsbereiche mit Bezug zum Datenschutz	37
A. Digitale-Inhalte-Richtlinie und nationale Umsetzung in §§ 327 ff.	
BGB	39
I. Europarechtlicher Hintergrund – Zielsetzung –	
Datenschutzrechtliche Relevanz	39
II. Problemfelder mit datenschutzrechtlicher Relevanz	40
1. Vorbemerkung	40
2. Anwendungsbereich der §§ 327 ff. BGB	41
3. Datenbereitstellung als Gegenleistung	45
4. Der Mangelbegriff	47
5. Vertragsrechtliche Folgen der Ausübung von	
Datenschutzrechten	48
III. Einzelfälle	49
1. Aufruf einer Webseite als Vertragsschluss?	49
2. PUR-Modelle	49
3. Internetmeinungsumfrage	51
4. „Pay as you drive“	51

Inhaltsverzeichnis

5. Internet of Things (IoT)	51
B. Gesetz gegen den unlauteren Wettbewerb (UWG)	52
I. Allgemeines	52
II. Verhältnis des Belästigungsschutzes nach § 7 UWG zur DS-GVO	52
III. Abmahnfähigkeit von Datenschutzverstößen	55
1. Arten von Abmahnungen und relevante EuGH-Rechtsprechung	55
2. Abmahnung von Datenschutzverstößen nach UKlaG	55
3. Wettbewerbsrechtliche Abmahnung von Datenschutzverstößen	56
C. Überblick über EU-Datenakte	59
I. Allgemeines	59
II. Digital Services Act (DSA)	60
III. Digital Markets Act (DMA)	60
IV. Daten-Governance-Rechtsakt	61
1. Datenvermittlungsdienste	61
2. Datenaltruismus	63
3. Weiterverwendung von Daten öffentlicher Stellen	64
4. Verhältnis des DGA zur DS-GVO	64
5. Bewertung	65
V. Data Act	65
1. Zugang und Nutzung mit Blick auf nutzergenerierte Daten	66
2. Sonderregeln für öffentliche Stellen	66
3. Datenübertragbarkeit	66
4. Datensicherheit bei Zugriff durch Drittstaaten und Einschränkung der Regelungen zum Datenteilen für „Gatekeeper“	66
5. Rechtsdurchsetzung	67
6. Verhältnis des DA zu anderen Rechtsakten	67
7. Bewertung	67
Teil B. Websites und Apps	
Kapitel 5. Funktionsweise und technische Erläuterungen	69
A. Einführung	69
B. Allgemeines zur Funktionsweise des Internets	70
I. Generelle Struktur und Aufbau	70
II. Protokolle	71
1. Protokollschichten	72
2. Zusammenspiel der Protokolle	75
3. Anwendungsprotokolle	75
III. Wesentliche Konzepte, Komponenten und Organisation	79
1. Routing	79
2. Content Delivery Netzwerke	79
3. Proxys	80
4. Domains und URLs	81
5. Domain Name System	82
6. Browser und Betriebssysteme	84
7. Cookies/Speicherung im Browser	86
8. Sicherheitsmodel des Webs	87
9. 1st und 3rd Partys	88

10. Organisation	89
IV. Sicherheit, Integrität und Authentizität	89
1. Domain Name System	90
2. Transport Layer Security	91
3. Ende-zu-Ende/Punkt-zu-Punkt	92
C. Einbindung externer Dienste	93
D. Apps	94
I. Besonderheiten im Vergleich zu herkömmlichen Applikationen	94
II. Native Apps, Hybride Apps und PWA	95
Kapitel 6. Zugriff und Speicherung von Informationen auf Endeinrichtungen	97
A. Allgemeines	98
I. Endnutzer	98
II. Informationen iSd § 25 TDDDG/ePrivacy-RL	99
III. Endeinrichtung	100
IV. Zugriff/Speicherung	101
1. Speicherung	101
2. Zugriff	101
V. Adressat der Norm	104
B. Tracking	105
I. Begriffsbestimmung	105
II. Technische Verfahren	106
1. Web-Beacons und Tracking-Pixel	106
2. Newsletter-Tracking	106
3. Script-basiertes Tracking	107
4. Cookie-Synching	108
5. Redirect basiertes Tracking	109
6. Fingerprinting	109
7. Mobile AdIDs	110
8. Offline-Tracking	110
9. Geolokalisierung/Geo-Targeting	110
C. Ausblick	111
I. Tracking Prevention	111
1. Browser	111
2. Browser-Erweiterungen	112
II. Neue Tracking Verfahren/Schnittstellen	112
III. Keine ePrivacy-Verordnung	113
Kapitel 7. Datenkategorien	115
A. Einleitung: Datenkategorien im Datenschutzrecht	115
B. Personenbezogene Daten	116
I. Begriffsdefinition nach Art. 4 Nr. 1 DS-GVO	116
1. Persönlicher Schutzzumfang: natürliche Person	117
2. Sachlicher Schutzzumfang: Information und Identifizierbarkeit	117
3. Anwendungsbeispiele	119
II. Pseudonyme Daten und Art. 4 Nr. 5 DS-GVO	120
1. Begriffsdefinition der Pseudonymisierung nach Art. 4 Nr. 5 DS-GVO	120
2. Anforderungen an Pseudonymität von Daten	121
3. Anwendungsbeispiele	121
C. Besondere Arten personenbezogener Daten nach Art. 9 DS-GVO	122
I. Sensible Daten nach Art. 9 Abs. 1 DS-GVO	122

Inhaltsverzeichnis

II. Besondere Zweckbestimmung oder Verwertungsabsicht?	122
III. Anwendungsbeispiele	123
D. Nicht personenbezogene Daten	123
I. Sach- und Maschinendaten	124
II. Anonymisierung und anonyme Daten	124
Kapitel 8. Datenschutzrechtliche Rolle der Beteiligten	127
A. Einführung	128
B. Das Rollenkonzept der DS-GVO im Einzelnen	129
I. Überblick	129
II. Abgrenzung zwischen Auftragsverarbeitung und alleiniger/gemeinsamer Verantwortlichkeit	132
1. Allgemeines	132
2. Abgrenzung Verantwortlichkeit (Art. 4 Nr. 7 DS-GVO) und Auftragsverarbeitung (Art. 28 DS-GVO)	134
3. Datenschutzrechtliche Anforderungen im Fall der Auftragsverarbeitung	137
4. Rechtsfolgen und Haftung im Fall der Auftragsverarbeitung	141
5. Beispiele für Auftragsverarbeitungen im Zusammenhang mit Onlineangeboten	142
6. Abgrenzung alleinige und gemeinsame Verantwortlichkeit	143
7. Rechtsfolgen und Pflichten im Fall der gemeinsamen Verantwortlichkeit	149
8. Verhältnis von gemeinsamer Verantwortlichkeit und Zweckänderung	153
9. Haftung im Fall der gemeinsamen Verantwortlichkeit	154
10. Beispiele für eine gemeinsame Verantwortlichkeit im Onlinebereich	154
III. Besonderheiten bei Drittlandbezug	159
C. Das Rollenkonzept des § 25 TDDDG	160
Kapitel 9. Erlaubnistatbestände der Datenverarbeitungen	163
A. Gesetzliche Erlaubnisse nach TDDDG	168
I. Verkehrsdaten: Dienstleistung (§ 9 TDDDG)	168
1. Anwendungsbereich und Legaldefinition der Verkehrsdaten (§ 3 Nr. 70 TKG)	168
2. Normadressaten – Verpflichtete nach § 3 Abs. 2 S. 1 TDDDG	170
3. Erlaubte Verarbeitungen	170
4. Löschpflicht unverzüglich nach Verbindungsende (§ 9 Abs. 1 S. 2 TDDDG)	171
5. Öffnungsklausel für spezialgesetzliche Verkehrsdatenverarbeitung (§ 9 Abs. 1 S. 4 TDDDG)	171
6. Einwilligungsvorbehalt für bestimmte Verarbeitungszwecke (Marketing, Angebotsoptimierung und Dienste mit Zusatznutzen)	172
7. Hinweispflicht bzgl. Einwilligungswiderruf (§ 9 Abs. 2 S. 5 TDDDG)	172
II. Standortdaten: Bereitstellung von Diensten mit Zusatznutzen (§ 13 TDDDG)	172
1. Standortdaten	173
2. Nutzer	174

3. „Dienst mit Zusatznutzen“	174
4. Erlaubnistatbestand: Einwilligungserklärung	174
5. Erlaubnistatbestand: Anonymisierung	175
6. Textmitteilung über Feststellung des Standortes	175
7. Einzelfalluntersagung der Verarbeitung durch Nutzer nach Einwilligung	176
8. Sonderregelungen bei Notrufnummern	176
III. Schutz der Privatsphäre bei Endeinrichtungen (§ 25 TDDDG)	176
1. Anwendungsbereich von § 25 TDDDG und Verhältnis zum Datenschutzrecht	176
2. Grundsatz: Einwilligungserfordernis (§ 25 Abs. 1 TDDDG)	180
3. Ausnahmen vom Einwilligungserfordernis (§ 25 Abs. 2 TDDDG)	181
4. Datenschutz	189
5. Rechtslage bei Mehrzweckcookies	189
6. Folgen bei Verstößen gegen § 25 TDDDG	190
7. Verhältnis von § 25 TDDDG zum Digital Services Act (DSA)	190
B. Gesetzliche Erlaubnisse nach DS-GVO	191
I. Allgemeines	191
II. Vertragserfüllung; vorvertragliche Maßnahmen	191
1. Normzweck	191
2. Betroffene Person als Vertragspartei	192
3. Vertragsverhältnis	192
4. Erfüllung einer vertraglichen Leistungspflicht	193
5. Erforderlichkeit zur Vertragserfüllung	193
6. Zahlen mit Daten	195
7. Vorvertragliche Maßnahmen	196
8. Vertragserfüllung im Beschäftigungsverhältnis	196
9. Keine Kopplungsproblematik	197
10. Konkurrenzen	197
III. Erfüllung einer rechtlichen Verarbeitungspflicht	197
IV. Schutz lebenswichtiger Interessen	198
1. Lebenswichtige Interessen; Interessenträger	198
2. Konkurrenzen	199
V. Wahrnehmung öffentlicher Aufgaben; Ausübung öffentlicher Befugnisse	199
VI. Überwiegende Verarbeitungsinteressen	200
1. Berechtigtes Interesse; Interessenträger	201
2. Interessenverwirklichende Maßnahme	202
3. Erforderlichkeit der Verarbeitung	202
4. Gegeninteresse des Betroffenen	203
5. Kein Überwiegen des Gegeninteresses	205
6. Widerspruchsrecht; zwingendes berechtigtes Interesse	206
7. Informationspflicht, Art. 13 Abs. 1 lit. d und Art. 14 Abs. 2 lit. b DS-GVO	206
8. Besonderheiten bei Daten von Kindern	206
9. Konkurrenzen	207
10. Dokumentation; Darlegungs- und Beweislast	207

Inhaltsverzeichnis

C. Einwilligungsbasierte Datenverarbeitung	208
I. Rechtliche Anforderungen an die Einwilligung	208
1. Verhältnis von einwilligungsbasierter Datenverarbeitung und Verarbeitungen nach Art. 6 Abs. 1 S. 1 lit. b DS-GVO	208
2. Verhältnis der Einwilligung zur Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f DS-GVO	214
3. Gültigkeitsdauer einer wirksam erteilten Einwilligung	215
4. Rechtliche Anforderungen an die Einwilligung im Einzelnen	215
II. Einwilligungsmanagement	237
1. Datenmittler nach dem Daten-Governance-Rechtsakt	238
2. Anerkannte Dienste zu Einwilligungsverwaltung gem. § 26 TDDDG	239
3. Verhältnis zwischen anerkanntem Dienst und Datenmittler	241
4. Datenschutzrechtliche Verantwortlichkeiten	242
5. Technische und organisatorische Ausgestaltung der PIMS	242
6. Wirtschaftliche Bedeutung	245
III. Der IAB TCF 2.2 Standard	245
1. Das IAB und der Zweck des TCF	247
2. Rechtliches Regelwerk und die Terminologie des TCF 2.2	247
3. Technische Aspekte des Frameworks	249
4. Was berücksichtigt das IAB TCF nicht	250
5. Verantwortung des Publishers und die Unterschiede/Konfigurierbarkeit von CMPs	251
6. TCF 2.2 als technische und organisatorische Maßnahme	254
7. Aktuelle Entwicklungen	254
Kapitel 10. Rechtfertigung einzelner Verarbeitungszwecke	259
A. Einleitung	259
B. Bereitstellung und Durchführung des Dienstes	260
I. Rechtfertigung nach TDDDG	261
II. Rechtfertigung nach DS-GVO	263
C. Abrechnung	263
I. Zulässigkeit nach TDDDG	264
II. Zulässigkeit nach DS-GVO	264
D. Statistische Analyse	265
I. Zulässigkeit nach TDDDG	265
II. Zulässigkeit nach DS-GVO	267
E. IT-Sicherheit	268
I. Zulässigkeit nach TDDDG	269
II. Zulässigkeit nach DS-GVO	270
F. Update- und Patchmanagement	271
I. Zulässigkeit nach TDDDG	271
II. Zulässigkeit nach DS-GVO	272
G. Werbung und Werbefinanzierung mit Reichweitenmessung	272
I. Werbecookies im Allgemeinen	272
1. Zulässigkeit nach TDDDG	273
2. Zulässigkeit nach DS-GVO	274
II. Service-gegen-Daten-Modelle	274
H. Produktverbesserung/Produktentwicklung	275

Kapitel 11. Veröffentlichungen und Entscheidungen von Aufsichtsbehörden, Gremien und Gerichten	277
A. Veröffentlichungen der Aufsichtsbehörden und Gremien	278
I. Charakter der Veröffentlichungen	279
II. Bedeutung für den Betrieb von Webseiten und Apps	281
III. Stellungnahmen und Leitlinien des Europäischen Datenschutzausschusses und der Artikel-29-Datenschutzgruppe	282
IV. Orientierungshilfen und Empfehlungen der Aufsichtsbehörden	285
B. Behördliche Entscheidungen	292
C. Gerichtsentscheidungen	298
Kapitel 12. Einbindung von Fotografien	301
A. Fotografien und personenbezogene Daten	302
B. Fotos und Datenverarbeitung im Internet	303
C. Anwendungsbereich der DS-GVO und Fotos im Internet	304
D. Rechtsgrundlage der Verarbeitung von fotobezogenen Daten	304
I. Verhältnis von DS-GVO und §§ 22f. KUG	304
II. Die Einwilligung als Rechtsgrundlage, Art. 6 Abs. 1 lit. a DS-GVO	305
III. Vertrag als Rechtsgrundlage, Art. 6 Abs. 1 lit. b DS-GVO bzw. § 26 Abs. 1 S. 1 BDSG	307
IV. Berechtigtes Interesse als Rechtsgrundlage zum Fotografieren und zur Fotonutzung, Art. 6 Abs. 1 lit. f DS-GVO	308
V. Besondere Kategorien personenbezogener Daten bei Personenfotos, Art. 9 Abs. 1 DS-GVO	310
VI. Besonderheiten bei Fotodatenverarbeitungen durch Behörden	311
E. Pflichten im Zusammenhang mit der Fotodatenverarbeitung	311
I. Informationspflichten und Betroffenenrechte bei Fotodatenverarbeitung	311
II. Aufbewahrungsdauer und Pflicht zur Löschung von Fotos, Art. 17 DS-GVO	312
III. Vertrag zur Auftragsverarbeitung, Art. 28 DS-GVO	312
Kapitel 13. Drittlandtransfer	315
A. Vorliegen eines Drittlandtransfers	316
B. Zwei-Stufen-Prüfung	317
C. Nicht zulässige Übermittlungen	318
D. Angemessenheitsbeschluss der Kommission	319
E. Geeignete Garantien	320
I. Überblick	320
II. Empfänger in den Vereinigten Staaten	321
III. Verbindliche interne Datenschutzvorschriften	322
IV. Standarddatenschutzklauseln der Kommission	324
1. Genehmigungspflicht	324
2. Modularer Aufbau	325
3. Transfer Impact Assessment	325
V. Standarddatenschutzklauseln der Aufsichtsbehörden	327
VI. Standarddatenschutzklauseln von Verantwortlichen oder Auftragsverarbeitern	327
VII. Verwaltungsvereinbarungen	327
VIII. Verhaltensregeln	328

Inhaltsverzeichnis

IX. Zertifizierungsverfahren	328
F. Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO)	328
I. Ausdrückliche Einwilligung	328
II. Erfüllung eines Vertrages mit dem Betroffenen	329
III. Abschluss oder Erfüllung eines Vertrages im Interesse des Betroffenen	330
IV. Wahrung wichtiger öffentlicher Interessen	330
V. Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen	330
VI. Wahrung lebenswichtiger Interessen	331
VII. Datenübermittlung aus für die Öffentlichkeit bestimmten Registern	331
VIII. Zwingende berechtigte Interessen	331
Kapitel 14. Datensicherheit	333
A. Datenschutzrechtliche Grundlagen	333
B. Risikoermittlung, -analyse, -beurteilung und -behandlung sowie Sicherheit der Verarbeitung durch technische und organisatorische Maßnahmen	337
I. Ermittlung des Schutzniveaus	337
1. Art, Umfang, Zwecke und Umstände der Datenverarbeitung	338
2. Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen	338
3. Unterschied zwischen der Ermittlung des Schutzniveaus in der Informationssicherheit und im Datenschutz	340
II. Technische und organisatorische Maßnahmen unter Berücksichtigung der Risiken	341
1. Stand der Technik	342
2. Implementierungskosten	344
3. Auswahl technischer und organisatorischer Maßnahmen unter Berücksichtigung des Schutzniveaus, des Stands der Technik und der Implementierungskosten	344
4. Prüfung der Wirksamkeit	347
C. Privacy by Design und Privacy by Default	348
D. Genehmigte Verhaltensregeln und Zertifizierungen	349
E. Anerkannte Standards	349
I. ISO-Normen	350
II. IT-Grundschutz des BSI	351
Kapitel 15. Transparenz und Informationspflichten	353
A. Regelung der Transparenz in der DS-GVO	355
I. Transparenz als Grundprinzip	355
II. Spezielle Transparenzregelungen	355
III. Adressaten der Transparenzpflicht	355
IV. Rechtsnatur der Transparenzinformationen	356
V. Rechenschafts- und Nachweispflichten	356
VI. Rechtsfolgen von Transparenzverstößen	357
1. Verhängung von Bußgeldern	357
2. Wettbewerbsrechtliche Ansprüche	357
3. Ansprüche der Betroffenen	357
4. Rechtswidrigkeit der Verarbeitung	358

B. Inhalte der Informationspflichten 358

 I. Informationspflichten bei der Direkterhebung von Daten 358

 1. Name und Kontaktdaten des Verantwortlichen und ggf. Vertreters 359

 2. Kontaktdaten des Datenschutzbeauftragten 359

 3. Zwecke und Rechtsgrundlage 359

 4. Berechtigte Interessen 360

 5. Empfänger oder Kategorien von Empfängern 360

 6. Beabsichtigte Übermittlung an ein Drittland 361

 7. Speicherdauer 361

 8. Betroffenenrechte 361

 9. Widerrufsrecht 362

 10. Beschwerderecht bei einer Aufsichtsbehörde 362

 11. Pflicht zur Bereitstellung der erhobenen Daten 362

 12. Automatisierte Entscheidung einschließlich Profiling 362

 II. Informationsgehalte bei indirekter Erhebung 363

 1. Kategorien personenbezogener Daten 363

 2. Beabsichtigte Übermittlung an Empfänger im Drittland 363

 3. Angabe der Datenquellen 364

 4. Pflicht zur Bereitstellung der erhobenen Daten 364

 III. Unbenannte Informationen 364

C. Zeitpunkt der Bereitstellung von Informationen 365

 I. Zeitpunkt der Information bei Direkterhebung 365

 II. Zeitpunkt der Information bei indirekter Erhebung 366

D. Informationspflichten bei nachträglichen Änderungen 366

 I. Zweckänderung nach direkter oder indirekter Erhebung 366

 II. Generelle Informationspflicht bei Änderungen 366

 III. Aktive Mitteilung 367

E. Ausnahmen von den Informationspflichten 367

 I. Ausnahme der Kenntnis bei Direkterhebung 367

 II. Ausnahmen bei indirekter Erhebung 368

 1. Kenntnis der Information 368

 2. Unmöglichkeit der Information sowie unverhältnismäßiger Aufwand 368

 3. Ausdrückliche Regelung durch Rechtsvorschriften der Union 368

 4. Daten unterliegen dem Berufsgeheimnis 369

 III. Nationale Ausnahmen im Rahmen von Öffnungsklauseln 369

F. Art und Form der Informationsvermittlung 370

 I. Präzise Informationen 370

 II. Leichte Zugänglichkeit 370

 1. Einfache Erkennbarkeit 370

 2. Unmittelbare Erreichbarkeit 371

 3. Medienbruch 371

 4. Kosten 372

 III. Verständlichkeit 372

 1. Maßgeblichkeit persönlicher und sachlicher Umstände 372

 2. Minderjährige und beeinträchtigte Personen 373

 IV. Klare und einfache Sprache 373

 1. Landessprache 373

 2. Bedingungsfeindlichkeit und Modalitäten 374

 V. Form und Gestaltung der Informationsvermittlung 374

 1. Schrift- und andere Form 375

Inhaltsverzeichnis

2. Mündliche Informationen	375
3. Visualisierung und Bildsymbole	375
4. Gestaltung der Informationsvermittlung	375
5. Kontextualität und das Mehrebenen-Modell	376
Kapitel 16. Initiativrechte der betroffenen Personen	379
A. Überblick	380
B. Modalitäten	382
I. Allgemeine Voraussetzungen	382
1. Willenserklärung	382
2. Frist	383
3. Untätigbleiben	384
4. Entgelt	386
5. Maschinenlesbare Bildsymbole	386
II. Internetspezifische Vorgaben	387
1. Kontaktaufnahme	387
2. Form und Formate	388
3. Datensicherheit	389
C. Die Rechte im Einzelnen	390
I. Auskunft	390
1. Negativauskunft	390
2. Metadaten	391
3. Inhaltsdaten	392
4. Ausnahmen	393
5. Konkurrenzen	394
II. Datenübertragbarkeit	394
1. Inhalt	394
2. Ausnahmen	395
III. Berichtigung und Vervollständigung	395
1. Inhalt	395
2. Ausnahmen	396
3. Konkurrenzen	396
IV. Löschung und Recht auf Vergessenwerden	396
1. Inhalt	396
2. Ausnahmen	397
3. Konkurrenzen	398
V. Einschränkung der Verarbeitung	398
VI. Widerspruch	398
1. Inhalt	398
2. Ausnahmen	399
3. Konkurrenzen	399
VII. Widerruf der Einwilligung	399
D. Rechtsdurchsetzung	400
I. Gerichtliche Geltendmachung	400
II. Behördliche Abhilfebefugnisse und Vollstreckung	401
E. Haftung	401
I. Schadensersatzforderung	401
II. Bußgeld	402
III. Verwarnung	402
IV. Beanstandung	402

Kapitel 17. Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen	403
A. Einleitung	405
I. Intention von Melde- und Benachrichtigungspflichten bei Datenschutzverletzungen	405
II. Besondere Relevanz für den Datenschutz im Internet	406
1. Grundlegende Schwachstellen in IT-Systemen	406
2. Durchdringung der Lebensbereiche mit vernetzter Technik	407
3. Datenschutzverletzungen bei Nutzung des Internets	408
4. Datenschutzverletzungen durch aktives Angreifen per Internet	409
5. Datenfunde im Internet	409
6. Reale Bedrohung	410
III. Entwicklung der Gesetzgebung	410
1. Vorgängerregelungen zu Art. 33 DS-GVO	410
2. Bezüge zu sonstigen Regelungen im Datenschutzrecht	411
3. Meldepflichten im Bereich der Netz- und Informationssicherheit	412
B. Allgemeines	413
I. Definition einer Verletzung des Schutzes personenbezogener Daten	413
1. Verletzung der klassischen Schutzziele der Informationssicherheit	413
2. Einordnung weiterer Datenschutzverletzungen	415
II. Pflichten des Verantwortlichen	416
1. Erkennen von Verletzungen des Schutzes personenbezogener Daten	416
2. Bewerten des Risikos für die Rechte und Freiheiten natürlicher Personen	417
3. Maßnahmen des Verantwortlichen nach einer Verletzung des Schutzes personenbezogener Daten	419
4. Dokumentation im Sinne der Rechenschaftspflicht	420
C. Art. 33 DS-GVO: Meldepflicht bei der zuständigen Aufsichtsbehörde	421
I. Entstehen der Meldepflicht und Ausnahmen von der Pflicht	421
II. Normadressat	421
1. Auftragsverarbeitung	422
2. Gemeinsame Verantwortlichkeit	422
III. Zuständige Aufsichtsbehörde	423
1. Innerdeutsche Fälle	423
2. Internationale Fälle	423
3. Außereuropäische Fälle	424
IV. Fristen	424
1. Meldung des Verantwortlichen an die Aufsichtsbehörde	424
2. Meldung eines Auftragsverarbeiters an den Verantwortlichen	425
V. Inhalt und Form der Meldung nach Art. 33 DS-GVO	425
VI. Besonderheiten im BDSG für den Bereich Polizei und Justiz	426
VII. Besonderheiten für den Bereich der Telekommunikation	426

Inhaltsverzeichnis

D. Art. 34 DS-GVO: Benachrichtigung der von einer Datenschutzverletzung betroffenen Person	428
I. Entstehen der Benachrichtigungspflicht und Ausnahmen von der Verpflichtung	428
1. Vorliegen eines hohen Risikos: grundsätzliche Benachrichtigungspflicht	428
2. Ausnahmen von der Benachrichtigungspflicht nach der DS-GVO	430
3. Ausnahmen von der Benachrichtigungspflicht nach BDSG	430
II. Normadressat	430
III. Fristen	431
IV. Inhalt und Form der Benachrichtigung nach Art. 34 DS-GVO	431
V. Information der betroffenen Personen auch ohne Vorliegen eines hohen Risikos	431
VI. Besonderheiten im BDSG für den Bereich Polizei und Justiz	432
VII. Besonderheiten im TKG	433
E. Empfehlungen für die Praxis	433
I. Prävention: Datenschutzverletzungen vermeiden	433
II. Vorbereitung: Datenschutzverletzungen erkennen können	434
III. Planung: Reaktion auf eventuelle Datenschutzverletzungen	434
IV. Training: Umgang mit Datenschutzverletzungen üben	435
V. Evaluation: Aus Datenschutzverletzungen lernen	436
Kapitel 18. Rechenschaftspflicht („Accountability“)	439
A. Sinn und Zweck der Rechenschaftspflicht	439
B. Konkretisierung der Rechenschaftspflicht	440
C. Umsetzung der Rechenschaftspflicht bei Internetangeboten	441
I. Künftige Datenverarbeitung rechtmäßig gestalten	441
II. Systematische Bewertung	442
D. Bedeutung der Rechenschaftspflicht bei behördlichen Maßnahmen	442
I. Umfang des Amtsermittlungsgrundsatzes	443
II. Untersuchungsbefugnisse gemäß Art. 58 Abs. 1 DS-GVO	444
III. Mitwirkungspflichten des Verantwortlichen und Auftragsverarbeiters	445
IV. Bußgeldtatbestand	448
E. Umfang und praktische Umsetzung der Rechenschaftspflicht/Einzelbereiche	449
I. Datenschutzrechtliche Rolle der Beteiligten	449
II. Einwilligung	450
1. Einwilligungen per E-Mail	450
2. Einwilligungen auf Websites	451
3. Differenzierte Betrachtung und Einzelfälle	451
III. Vertrag	453
1. Vertragsschluss	453
2. Verarbeitung für die Erfüllung	453
3. Erforderlichkeit	453
4. Anwendbare AGB	454
5. Werbung auf Basis der Rechtsgrundlage Vertrag	454
IV. Einbindung von Drittanbietern	455
1. Konfiguration von Tracking-Tools	455

2. Versionsverlauf von Websites/Apps	455
3. Einwilligungsmanagement	456
4. Datenschutzerklärung	456
Teil C. Spezifische Anwendungsszenarien	
Kapitel 19. Messenger	457
A. Technischer und netzökonomischer Hintergrund	458
I. Messenger als OTT-Dienste	458
II. Nutzungsverhalten und Nutzungsintensität von OTT-Diensten	458
III. Messenger: Angebotstypologie	459
B. Rechtlicher Rahmen	460
C. Elektronische Kommunikationsdienste und maßgebliche Bestimmungen	461
I. Begriffsbestimmungen in TDDDG und TKG	461
1. Interpersonelle Kommunikationsdienste	461
2. Gewöhnlich gegen Entgelt erbracht	461
3. Direkter interpersoneller und interaktiver Informationsaustausch	462
4. Zwischen einer endlichen Zahl von Personen	462
5. Negativabgrenzung: interpersonelle Kommunikation als lediglich untergeordnete Nebenfunktion	462
6. Nummerngebundene und nummernunabhängige interpersonelle Telekommunikationsdienste	463
II. Funktionale Bestimmung des anzuwendenden Datenschutzrechts	463
1. Große Gruppenchats und die Abgrenzung zu sozialen Netzwerken	464
2. § 3 Nr. 24 TKG aE und der Facebook Messenger	464
III. Fernmeldegeheimnis und Schutz einzelner Datenkategorien bei der Nutzung von Messengern	464
1. Fernmeldegeheimnis, § 3 Abs. 1 TDDDG	465
2. Verschlüsselte Inhalte	465
3. Staatliche Eingriffsbefugnisse	466
4. Staatlicher Zugriff auf Inhalte bei verschlüsselter Kommunikation	466
5. Nachrichtenübermittlung mit Zwischenspeicherung, § 6 TDDDG	467
6. Verkehrsdaten, § 9 TDDDG	468
7. Standortdaten, § 13 TDDDG	468
8. Bestandsdaten, § 21 TDDDG	469
9. Adressbuchdaten	469
10. Metadaten	471
D. Einzelfragen bestimmter Dienste in spezifischen Anwendungskontexten	472
I. WhatsApp und öffentliche Stellen	472
II. WhatsApp im Unternehmen	473
III. Messenger im Krankenhausbereich	473
E. Vorschlag für eine Verordnung zur Festlegung von Vorschriften für die Prävention und Bekämpfung des sexuellen Missbrauchs von Kindern („Chatkontrolle“)	474
I. Entwurf der Kommission vom 11.5.2022	474

Inhaltsverzeichnis

II. Rechtliche Würdigung	475
Kapitel 20. Einsatz von Social Media im Unternehmen	477
A. Beschäftigtendatenschutz	480
I. Pre-Employment-Screening	480
1. Begriffsbestimmung und Reichweite	480
2. Datenschutzrechtliche Zulässigkeit	481
3. Betroffenenrechte	484
4. Mögliche Folgen unberechtigter Auswertungen	484
II. Social Media Guidelines	485
1. Begriffsbestimmung und Anwendungsgebiete	485
2. Möglichkeiten zur Implementierung einer Social Media Guideline	486
3. Implementierung als Policy oder als Guideline	486
4. Mögliche Inhalte & Regelungen	487
5. Folgen von Verstößen gegen Social Media Guidelines	487
6. Hinweise zur Erstellung von Social Media Guidelines	488
III. Sicherung von Arbeitgeberrechten an Social-Media-Kontakten	488
1. Einführung in die Problematik	488
2. Einzelheiten zu Rechten an Social Media	488
3. Herausgabe/Löschung von Daten	489
4. Empfohlene Maßnahmen zur Sicherung von Arbeitgeberrechten	490
IV. Unternehmensinterner Einsatz von Social Media	491
1. Begriffsbestimmung	491
2. Datenschutzrechtliche Zulässigkeit	491
3. Sicherung der Verarbeitungsgrundsätze aus Art. 5 Abs. 1 DS-GVO	494
4. Information der betroffenen Personen	494
5. Löschung von Mitarbeiterdaten	494
6. Mitbestimmung des Betriebsrats	495
7. Kein Konzernprivileg und Verantwortlichkeit	496
8. Übermittlungen in Drittländer	496
9. Nutzungsregeln für unternehmensinterne Social Media	497
B. Kunden-/Interessentendatenschutz	497
I. Kundenbindung/-service in sozialen Netzwerken	497
1. Begriffsbestimmungen	497
2. Datenschutzrechtliche Anforderungen	497
3. Wettbewerbsrechtliche Anforderungen	501
II. Kommunikation über Fanpages, zB Reaktion auf Lob oder Beschwerden	502
1. Begriffsbestimmung	502
2. Datenschutzrechtliche Zulässigkeit	502
3. Wettbewerbsrechtliche Aspekte	503
4. Betroffenenrechte	503
5. Aufbewahrungsfristen	504
III. Erhebung und Auswertung in anonymisierter Form zu Marktforschungszwecken	504
1. Begriffsbestimmung Anonymisierung	504
2. Anonymisierung als datenschutzrechtliche Verarbeitung und Zulässigkeit	505
3. Information der betroffenen Personen	507

4. Datenschutz-Folgenabschätzung	507
IV. Anreichern von Kundenprofilen mittels Informationen aus dem Internet	507
1. Begriffsbestimmung	507
2. Datenschutzrechtliche Zulässigkeit der Anreicherung von Kundenprofilen	507
3. Datenschutzrechtliche Zulässigkeit der (automatisierten) Anreicherung (Scraping)	509
4. Betroffenenrechte	509
5. Datenschutz-Folgenabschätzung	510
V. Social Media Marketing	510
1. Begriffsbestimmung	510
2. Datenschutzrechtliche Zulässigkeit	510
3. Betroffenenrechte	511
4. Datenschutz-Folgenabschätzung	511
5. Wettbewerbsrechtliche Anforderungen	512
VI. Online-Gewinnspiele	512
1. Begriffsbestimmung	512
2. Datenschutzrechtliche Zulässigkeit	512
3. Betroffenenrechte	513
C. Spezifische Anforderungen einzelner sozialer Netzwerke	514
I. Besonderheiten beim Einsatz von Facebook & Instagram	514
1. Verantwortlichkeit	514
2. Handlungsempfehlungen	515
3. Betroffenenrechte	515
4. Drittlandsübermittlungen	515
II. Besonderheiten beim Einsatz von X (vormals Twitter)	516
1. Verantwortlichkeit	516
2. Betroffenenrechte	517
3. Drittlandsübermittlungen	517
4. Sonstiges	517
III. Besonderheiten beim Einsatz von TikTok	517
1. Verantwortlichkeit	517
2. Drittlandsübermittlungen	517
IV. Besonderheiten beim Einsatz von LinkedIn	518
1. Verantwortlichkeit	518
2. Sonstiges	518
Kapitel 21. Datenbasierte Geschäftsmodelle im Online-Marketing	519
A. Digitale Geschäftsmodelle	522
I. Einleitung	522
II. Allgemeines zu datenbasierten Geschäftsmodellen	526
1. Daten als Grundlage einer Wertschöpfung	526
2. Tracking und Targeting	526
3. Tracking ohne Cookies	527
4. Reichweitenmessung	528
III. Datenbasierte Geschäftsmodelle im Einzelnen	529
1. Datenfinanzierte Geschäftsmodelle und Mischformen	529
2. Monetäres Geschäftsmodell Paid Content und Mischformen	529
3. Affiliate-Marketing	529
4. Werbenetzwerke	530
5. E-Mail-Marketing	532

Inhaltsverzeichnis

- IV. Werbefinanzierte Inhalte-Angebote von Medienunternehmen 534
- B. Datenschutzrechtliche Verantwortlichkeit 536
- C. Zulässigkeit von Verarbeitungen nach TDDDG und DS-GVO 537
 - I. Zusammenwirken von TDDDG und DS-GVO 537
 - II. Einwilligung vs. „unbedingte Erforderlichkeit“ 538
- III. Erlaubnistatbestände im Kontext der datenverarbeitenden Anwendungen 539
 - 1. Einwilligung 539
 - 2. Vertragliche Grundlage 540
 - 3. Berechtigtes Interesse 540
- IV. Anwendungsbeispiele aus der Praxis 541
- D. Profiling und automatisierte Entscheidungen, Art. 22 DS-GVO 542
- E. Wettbewerbsrechtliche Implikationen 544
 - I. Nebeneinander von UWG und DS-GVO 544
 - II. Übertragbarkeit datenschutzrechtlicher Anforderungen an eine Einwilligung zu Werbezwecken 545
 - 1. Unterschiedliche Schutzzwecke 545
 - 2. Terminologische Unterschiede bei der Konkludenten Einwilligung 546
 - 3. Bestimmtheit der Werbeeinwilligung 546
- III. Datenschutzrechtliche Aspekte im Zusammenhang mit der Bestandskundenwerbung 547
- IV. Sonstige wettbewerbsrechtliche Einflüsse bei datenverarbeitenden Anwendungen im Online-Marketing 548
- F. Gestaltung von Einwilligungs-Bannern 549
 - I. Aktualität und Relevanz 549
 - II. Anforderungen an die Wirksamkeit der Einwilligung 550
 - 1. Zeitpunkt 550
 - 2. Informiertheit 550
 - 3. Nachweis 552
 - 4. Eindeutige bestätigende Handlung des Nutzers 552
 - 5. Kopplung Einwilligung und Zugang zum Angebot (Art. 7 Abs. 4 DS-GVO) 553
 - 6. Widerruf der Einwilligung 554
- III. Praxisrelevante Fragen im Zusammenhang mit der Bannergestaltung 554
 - 1. Framing, Nudging und Dark Patterns 554
 - 2. Alles-Ablehnen-Button 557
 - 3. PUR-Modelle und Cookie-Walls 559
- G. Verfahren der belgischen Aufsichtsbehörde zum TCF 2.0 568
 - I. Kohärenzverfahren 568
 - II. Kernpunkte der Entscheidung der belgischen Aufsichtsbehörde 569
 - III. Inhalt und Stand des Verfahrens 570
 - IV. Aktualisierte Version des IAB-Standards – TCF 2.2 571
 - V. Ausblick 571
- H. Werbeblocker 572
 - I. Ausgangslage und BGH-Entscheidung „Werbeblocker“ 572
 - II. Datenschutzrechtliche Implikationen 573
- I. Blocker von Consent Management Plattformen 575
 - I. Ausgangslage 575

- II. Folgen des CMP-Blockings 576
 - 1. Datenschutzrechtliche Konsequenzen 576
 - 2. Wirtschaftliche Auswirkungen 577
 - III. Rechtmäßigkeit von CMP-Blockern 577
 - 1. Datenschutzrecht 577
 - 2. Wettbewerbsrecht/Zivilrecht 577
 - 3. Mögliche Urheberrechtsverletzungen 578
 - 4. Zulässigkeit von technischen Abwehrmaßnahmen gegen CMP-Blocker 578
 - J. Zusammenfassung und Ausblick 579
 - I. Bestehende Rechtsunsicherheit und Interessenlage 579
 - II. Ansätze zur Vereinfachung und Vereinheitlichung der Einwilligungseinholung 580
 - 1. Personal Information Management Systems – PIMS 581
 - 2. Sonstige Ansätze für softwarebasierte Unterstützung des Nutzers 582
 - 3. Compliance Tools 582
 - III. Verstärkter Fokus auf Vertrags- statt Einwilligungslösungen 583
 - IV. Zukunft der Werbenetzwerke 583
 - 1. Aktuelle Entwicklungen und alternative Technologien 583
 - 2. EDSA-Leitlinien 2/2023 zum technischen Anwendungsbereich von Art. 5 Abs. 3 ePrivacy-RL 585
- Kapitel 22. Recht des E-Mail-Marketings 587
 - A. Systematik und Zusammenspiel mit der DS-GVO 588
 - I. Wettbewerbsrecht und Deliktsrecht 588
 - II. Datenschutzrecht 589
 - III. „Wechselwirkung“ zwischen UWG und DS-GVO und Ausnahmen 590
 - B. Rechtsrahmen des E-Mail-Marketings 591
 - I. Begriff der Werbung 591
 - II. Elektronische Post 593
 - III. Grundsatz der Einwilligung 594
 - 1. Begriffe 594
 - 2. Wirksamkeitsvoraussetzungen 594
 - 3. Nachweis der Einwilligung 601
 - IV. Ausnahme für Werbung per elektronischer Post gegenüber Bestandskunden 604
 - 1. Allgemeines 604
 - 2. Tatbestandsvoraussetzungen von § 7 Abs. 3 UWG 604
 - C. Erfolgskontrolle und Personalisierung 610
 - I. Cookies, Pixeltags, Link-Tracking 610
 - II. Profilbildung 611
 - III. Gesonderte Einwilligung in Maßnahmen der Personalisierung? 612
 - D. Widerruf und Widerspruch, Verwirkung von Erlaubnistatbeständen 614
 - E. Abmahnungen, Ansprüche von Geschädigten und Sanktionsrisiken ... 617
 - I. Wettbewerbsrecht und Deliktsrecht 617
 - II. Datenschutzrecht 619
- Kapitel 23. Onlineshops 621
 - A. Einleitung 622
 - B. Anwendbares Recht 622

Inhaltsverzeichnis

C. Datenschutzrechtliche Verantwortlichkeit	622
I. Vertrieb über Online-Verkaufsplattformen	622
II. Betrieb eines eigenen Onlineshops	623
III. Hybride Vertriebsformen	625
D. Bestellung mit und ohne Kundenkonto	625
I. Kundenkonten und alternative Bestellmöglichkeiten	625
II. Anforderungen an Kundenkonten	626
1. Freiwilligkeit der Registrierung	626
2. Bestätigung im Wege des Double-Opt-In	626
3. Sperrung und Löschung von Kundenkonten	627
E. Datenverarbeitungen im Bestellprozess	627
I. Einsatz von Cookies	627
II. Datenerhebungen beim Entgegennehmen der Bestellung	628
1. Zwingend erforderliche Daten	628
2. Abfrage des Geschlechts	628
3. Abfrage des Geburtsdatums	629
III. Adressvalidierung/-verifizierung	630
IV. Bonitätsprüfung/Scoring	630
F. Einbindung von Dienstleistern und externen Partnern	631
I. Zahlungsdienstleister	632
II. Versanddienstleister	632
III. Forderungsmanagement und Inkasso	633
G. Behördliche Auskunftsverlangen	634
H. Kundenservice	634
I. Maßnahmen des Direktmarketings	635
I. Postalische Werbung	635
II. Werbemaßnahmen per E-Mail	635
III. Werbung gegenüber Gastbestellern	636
IV. Werbung gegenüber Warenkorbabbrechern	636
V. Bewertungsbitten und Kundenzufriedenheitsumfragen	637
VI. Umsetzung des Werbewiderspruchs	637
J. Informationspflichten	637
I. Allgemeine Anforderungen	637
II. Besonderheiten beim Vertrieb über Verkaufsplattformen	638
K. Technisch-organisatorische Maßnahmen	638
Kapitel 24. Computerspiele	641
A. Verarbeitungsprozesse und Rechtsgrundlagen	641
I. Kundenkonto	641
II. Bereitstellung des Dienstes	642
III. Käufe innerhalb des Spiels	642
IV. Produktverbesserung	643
V. Betrugs- und Cheatingprävention	644
VI. Interaktion zwischen Spielern (zB Chat)	645
VII. Werbung	646
B. Datenschutzrechtliche Rolle der Beteiligten	646
I. Developer/Publisher	646
II. Vertriebsplattformen	647
III. Zahlungsabwickler	648
Kapitel 25. Videokonferenzen – Einsatz im Beschäftigungsverhältnis	649
A. Abgrenzung TelKo – ViKo	650

B. Rechtliche Rahmenbedingungen	651
I. Telekommunikationsrechtliche Verantwortlichkeit	651
1. Kreis der Verpflichteten nach § 3 Abs. 2 S. 1 TDDDG	651
2. Verpflichtung nach § 3 Abs. 2 S. 1 Nr. 1 und 2 TDDDG	651
3. Geschützter Personenkreis	652
4. Rechtsfolge	653
5. Auswirkungen in der Praxis	653
II. Beschäftigten-Datenschutzrecht (DS-GVO und BDSG)	654
1. Erforderlichkeit	654
2. Einwilligung	657
3. Betriebsvereinbarungen	658
4. Exkurs	659
Kapitel 26. Datenschutz im Internet of Things	665
A. Einführung	665
B. Begriff des IoT und technische Grundlagen	666
C. Anwendbares Datenschutzrecht im IoT	668
D. IoT-Daten im Lichte der datenschutzrechtlichen Regelungen	669
I. Personenbezug als Ausgangspunkt der Betrachtung	669
II. Datenschutzrechtliche Verantwortlichkeit im IoT	670
III. Zulässigkeit der Datenverarbeitung im IoT	671
1. Zulässigkeit nach TDDDG	671
2. Zulässigkeit nach DS-GVO – Vertrag, Einwilligung und berechtigte Interessen	672
3. Werkzeug der Pseudonymisierung	673
4. Zulässige Weiterverarbeitung	673
E. Allgemeine Datenschutzprinzipien für vernetzte Endgeräte	675
F. Fazit und Ausblick	676
Kapitel 27. Connected Cars	679
A. Datensammlung in Fahrzeugen	680
I. Datenerfassung und Datentypen	680
II. Übertragungswege	680
B. Anwendbare Regelungen	681
I. Allgemeiner Datenschutz nach DS-GVO	681
II. Schutz der Geräteintegrität und Privatsphäre nach TDDDG	682
1. Speicherung von Informationen oder Zugriff auf gespeicherte Informationen	682
2. „Werkstattfälle“	683
3. Differenzierung nach Steuergeräten	683
III. Konkurrenzverhältnis TDDDG und DS-GVO	683
C. Rechtfertigung	684
I. DS-GVO	684
II. TDDDG	686
1. Nachrichtenübermittlung über TK-Dienst	686
2. Erbringung von digitalen Diensten	686
3. Einschränkung des Anwendungsbereichs: Pflichtenkollision	688
4. Einholung einer Einwilligung nach § 25 Abs. 1 TDDDG	688
5. Person des Einwilligenden	689
III. Zusammenspiel zwischen TDDDG und DS-GVO	690
Kapitel 28. Künstliche Intelligenz	691
A. Einführung	692

Inhaltsverzeichnis

- B. Begriff der künstlichen Intelligenz 693
 - I. Begriffsbestimmung in der KI-VO 693
 - II. Weitere Definitionsansätze 693
- C. KI-spezifische Regulierung in Deutschland und Europa 695
- D. Datenschutzrechtliche Regulierung 696
 - I. Europäischer Rechtsrahmen 696
 - 1. DS-GVO 696
 - 2. Verordnung über künstliche Intelligenz (KI-VO) 703
 - II. Nationale datenschutzrechtliche Regelungen 706
 - 1. BDSG und Landesdatenschutzgesetze 706
 - 2. Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) 706
 - 3. Medienstaatsvertrag (MStV) 707
- E. Bußgelder und Haftung 707
- Kapitel 29. Rechtskonformer Einsatz von KI-Sprachsystemen im Unternehmen 709
 - A. Einführung 710
 - B. Datenschutzrecht 711
 - I. Kategorien personenbezogener Daten 711
 - 1. Trainingsdaten 711
 - 2. Betriebsbezogene Eingabedaten 712
 - 3. Sonstige Eingabedaten 713
 - II. Verantwortlichkeit 713
 - 1. Verantwortlichkeit für die Verarbeitung von Trainingsdaten 713
 - 2. Verantwortlichkeit für die Verarbeitung von betriebsbezogenen Eingabedaten 714
 - 3. Verantwortlichkeit für die Verarbeitung von sonstigen Eingabedaten 714
 - III. Rechtsgrundlage 715
 - 1. Verarbeitung einfacher Kategorien personenbezogener Daten 715
 - 2. Verarbeitung besonderer Kategorien personenbezogener Daten 717
 - 3. Anforderungen an die Einwilligung in eine Verarbeitung der betriebsbezogenen Eingabedaten 717
 - 4. Widerruf der Einwilligung 718
 - IV. Betroffenenrechte 718
 - 1. Informationspflichten 718
 - 2. Geltendmachung der Rechte in Art. 15 ff. DS-GVO 719
 - V. Schutz der Privatsphäre bei Endeinrichtungen 719
 - C. Weitere Rechtsfragen 720
 - I. Rechtsverletzungen beim Einsatz von KI-Sprachsystemen 720
 - 1. Verantwortlichkeit des Nutzers 720
 - 2. Verpflichtung der Anbieter 721
 - 3. Konsequenzen für Unternehmen 722
 - II. Urheberrecht 722
 - 1. Zulässigkeit des Trainings 722
 - 2. Zulässigkeit der Nutzung der Ergebnisse 723
 - 3. Schutz der generierten Ergebnisse 723
 - D. Ausblick: KI-Verordnung 724
 - I. Risikobasierter Ansatz 724
 - II. Regulierung von GPAI-Modellen 725

III. Transparenzanforderungen an KI-Sprachsysteme	726
E. Zusammenfassung der Ergebnisse und Fazit	726
Kapitel 30. Digitaler Nachlass	729
A. Der digitale Nachlass und postmortaler Datenschutz	730
I. Das digitale Erbe	730
II. Der postmortale Datenschutz	730
B. Vererbbarkeit von Accountverhältnissen nach den §§ 1922 ff. BGB	731
I. Der Anspruch auf Zugangsgewährung	731
1. Kein individueller Zuschnitt der Leistung	
„Zugangsgewährung“	732
2. Inhalt des Anspruchs auf Zugangsgewährung	733
II. Einsichtsrecht der Erben in die digitale Kommunikation	733
1. Das postmortale Persönlichkeitsrecht des Kontoinhabers	733
2. Das Fernmeldegeheimnis	734
III. Recht zur aktiven Weiternutzung	735
1. BGH-Rechtsprechung zu Giroverträgen	735
2. Das Merkmal der Individualisierung der	
Leistungsbeziehung	736
3. Ergebnis: Regelmäßig keine Vererbbarkeit von	
Benutzeraccounts auf sozialen Netzwerken	737
4. Das postmortale Persönlichkeitsrecht des Erblassers	738
C. Die Anforderungen der DS-GVO und der Übergang digitaler Rechte	
im Todesfall	738
I. Datenverarbeitung durch die Anbieter von	
Online-Plattformen	738
II. Datenverarbeitungen durch die Erben als Verantwortliche	739
III. Datenverarbeitungen durch „digitale Nachlassverwalter“	739
D. Empfehlungen für den Vorsorge- und Erbfall	740
I. Vorsorge zu Lebzeiten	740
II. Vorsorge für den Todesfall	742
1. Zu berücksichtigende Interessen von Erblassern und	
Erben	742
2. Vorsorgeinstrumente	742
III. Vorsorgeangebote der Dienstanbieter und Dritter	745
1. Lösungsangebote der Dienstanbieter	745
2. Abwicklung durch kommerzielle Anbieter	746
IV. Fazit	747
Kapitel 31. Internetdaten und Sicherheitsbehörden	749
A. Einführung	750
I. Überblick Internetdaten, Sicherheitsbehörden und betroffene	
Datenarten	751
1. Internetdaten	751
2. Sicherheitsbehörden	751
3. Betroffene Datenarten	751
II. Prinzip der Doppeltür	752
III. Betroffene Grundrechte und verfassungsrechtliche	
Verhältnismäßigkeitsanforderungen an Eingriffsrechte	752
IV. (Subsidiär) zu beachtendes Datenschutzrecht	753
1. Telemedien/Digitale-Dienste- und	
Telekommunikationsanbieter	753
2. Sicherheitsbehörden	753

B. Datenerhebung beim Anbieter	754
I. Sicherstellung, Beschlagnahme, Auskunfts- und Herausgabeersuchen	754
1. Allgemeines	754
2. Abrufnormen	755
3. Übermittlungsnormen	755
4. Verfahren	756
5. Sonstiges, Besonderheiten, Kritik	756
II. Bestands- und Zugangsdatenauskunft, auch anhand von IP-Adressen, im TK-Bereich	757
1. Allgemeines	757
2. Abrufnormen	758
3. Übermittlungsnormen	759
4. Verfahren	760
5. Sonstiges, Besonderheiten, Kritik	760
6. Sonderfall: automatisiertes Auskunftsverfahren	760
III. Bestands- und Zugangsdatenauskunft, auch anhand von IP-Adressen, im Telemedien-/Digitale-Dienste-Bereich	761
1. Allgemeines	761
2. Abrufnormen	762
3. Übermittlungsnormen	763
4. Verfahren	763
5. Sonstiges, Besonderheiten, Kritik	764
IV. Verkehrsdatenauskunft	764
1. Allgemeines	764
2. Abrufnormen	764
3. Übermittlungsnormen	765
4. Verfahren	765
5. Sonstiges, Besonderheiten, Kritik	766
6. Sonderfall: Vorratsdatenspeicherung	766
V. Nutzungsdatenauskunft	767
1. Allgemeines	767
2. Abrufnormen	767
3. Übermittlungsnormen	767
4. Verfahren	768
5. Sonstiges, Besonderheiten, Kritik	768
VI. Sonderfall: proaktive Übermittlungspflichten sozialer Netzwerke	768
C. Datenerhebung während des Übertragungsvorgangs	769
I. TKÜ	769
1. Allgemeines	769
2. Abrufnormen	769
3. Verfahren	770
4. Sonstiges, Besonderheiten, Kritik	770
II. WLAN-Catcher	770
III. Strategische Überwachung des Internetverkehrs	770
D. Datenerhebung bei den Beteiligten der Kommunikation	771
I. Quellen-TKÜ	771
1. Allgemeines	771
2. Abrufnormen	772
3. Verfahren	772
4. Sonstiges, Besonderheiten, Kritik	772
II. Online-Durchsuchung	773

E. Weitere Formen der Datenerhebung	774
I. Erhebung offener Daten im Internet	774
II. Zugriff auf zugangsgesicherte (Kommunikations-)Inhalte im Internet	774
III. Datenerhebung in Chats und Foren unter falschen Angaben	775
F. Kernbereichsschutz	775
G. Informations-, Auskunfts- und Benachrichtigungspflichten	776
H. Rechtsschutzmöglichkeiten	776
I. Zusammenfassung, Kritik und Ausblick	778
 Teil D. Risiken bei Datenschutzverstößen	
Kapitel 32. Unterlassungsansprüche	781
A. Einführung	783
B. Überblick über Unterlassungsansprüche im datenschutzrechtlichen Rechtsschutzsystem	783
I. Vorgerichtliches Vorgehen	783
1. Abmahnung	783
2. Unterlassungs- und Verpflichtungserklärung	784
II. Überblick: Rechtsschutz für Betroffene, Verbände und Mitbewerber	785
1. Individualrechtsschutz	786
2. Kollektivrechtsschutz	786
3. Mitbewerberrechtsschutz	787
III. Besonderheiten im einstweiligen Rechtsschutz	789
C. Individualklagen auf Unterlassung	791
I. Verhältnis der DS-GVO zu Rechtsbehelfen aus dem nationalen Recht	791
II. Internationale, sachliche und örtliche Zuständigkeiten	793
III. Anspruchsgrundlagen für Unterlassungsansprüche	794
1. Originärer Unterlassungsanspruch aus Art. 17 DS-GVO	794
2. Quasinegatorischer Unterlassungsanspruch aus § 823 Abs. 2 iVm § 1004 Abs. 1 BGB analog iVm § 25 Abs. 1 TDDDG	795
3. Quasinegatorischer Unterlassungsanspruch aus § 823 Abs. 2 iVm § 1004 Abs. 1 BGB analog iVm Art. 6 Abs. 1 DS-GVO	797
4. Quasinegatorischer Unterlassungsanspruch aus § 823 Abs. 1 iVm § 1004 Abs. 1 BGB analog iVm Allgemeinem Persönlichkeitsrecht	797
5. Negatorischer Unterlassungsanspruch wegen Eigentumsbeeinträchtigung aus §§ 823 Abs. 1, 1004 BGB	799
6. Possessorischer Unterlassungsanspruch aus § 858 Abs. 1, § 862 Abs. 2 BGB	799
D. Kollektivklagen auf Unterlassung	799
I. Verbandsklagen nach dem UKlaG	799
1. Aktivlegitimation	800
2. Passivlegitimation	803
3. Internationale, sachliche und örtliche Zuständigkeit der Gerichte	803
4. Anhörung der zuständigen inländischen Aufsichtsbehörde ...	804
II. Verbandsklagen nach dem UWG	805

Inhaltsverzeichnis

E. Praxishinweise	807
I. Beweis- und Darlegungslast im Zivilprozess	807
II. Typisierende Beweismittel bei Unterlassungsklagen	808
III. Anforderung an die Bestimmtheit von Klageanträgen	809
IV. Rechtsschutzbedürfnis	811
V. Vollstreckung	811
F. Musterformulierung: Klage auf Unterlassung der Nutzung von Cookies	812
G. Ausblick	814
I. Keine Rechtsbehelfe nach der ePrivacy-Verordnung	814
II. Verbandsklagerichtlinie (Richtlinie (EU) 2020/1828)	814
Kapitel 33. Schadensersatz	817
A. Allgemeines	818
B. Schadensersatz nach Art. 82 DS-GVO	818
I. Anspruchsvoraussetzungen	819
1. Darlegungs- und Beweislast	819
2. Verstoß gegen die Verordnung	821
3. Schaden	821
4. Verschulden	823
5. Kausalität	824
6. Grundsätze der Schadensbemessung	825
II. Besonderheiten bei der Auftragsverarbeitung und der gemeinsamen Verantwortlichkeit	826
1. Besonderheiten bei der Auftragsverarbeitung	826
2. Grundsätze der Haftung bei der Beteiligung mehrerer Stellen	827
III. Geltendmachung von DS-GVO-Schadensersatz in der Praxis	828
1. Überblick über aktuelle Rechtsprechung zu Art. 82 DS-GVO	828
2. Aktuelle Rechtsprechung zu Datenpannen im Internet	829
3. Ausblick auf weitere Entwicklung der Rechtsprechung	830
4. Risiko von Massenklagen	831
IV. Verteidigung gegen DS-GVO-Schadensersatzforderungen	831
Kapitel 34. Aufsichtliches Verfahren	833
A. Zuständigkeit	834
B. Verfahren	836
C. Form	838
D. Aufgaben und Befugnisse	838
E. Verteidigungsstrategien und Handlungsempfehlungen	839
I. Informiertheit	839
II. Interne Prüfung	839
III. Kooperation	840
IV. Konfliktstrategie	840
V. Rechtsrat	840
VI. Rechtsschutz	840
VII. Schadensersatz	841
Kapitel 35. Bußgeldverfahren	843
A. Verhältnis zum aufsichtsbehördlichen Verwaltungsverfahren	844
B. Verfahren	845
I. Maßgebliches Verfahrensrecht	845
II. Zuständigkeit	845

III. Untersuchungsbefugnisse	846
IV. Offenlegungspflichten und Selbstbelastungsfreiheit	846
V. Form	847
C. Bußgeldadressat	847
I. Verantwortliche/Auftragsverarbeiter	848
II. Verhaltenszurechnung	848
III. Nebentäterschaft	850
IV. Datenschutzbeauftragter	850
D. Materieller Bußgeldtatbestand	850
I. Verstöße nach Art. 83 Abs. 4 DS-GVO	851
II. Verstöße nach Art. 83 Abs. 5, 6 DS-GVO	851
III. Verstöße gegen nationale Vorschriften	852
IV. Verschulden	852
V. Versuch	853
VI. Verjährung	853
E. Bußgeldentscheidung	853
I. Entscheidung über das „Ob“	853
II. Entscheidung über die Bußgeldhöhe	854
III. Unternehmensbegriff	855
IV. Bußgeldkriterien	856
V. Konzept der DSK	856
VI. Haftung der Muttergesellschaft und Regress	858
VII. Zahlungserleichterung	859
F. Behördliche Öffentlichkeitsarbeit	860
G. Rechtsschutz	860
H. Rechtskräftiges Bußgeld	861
Stichwortverzeichnis	863