

Inhaltsverzeichnis

Vorwort der Herausgeber	15
Vorwort zur 1. Auflage	19
Geleitwort.....	21
Grußwort.....	29
Autorenverzeichnis.....	31
Abkürzungsverzeichnis	33
Literaturverzeichnis	41
1. Einführung in den gesamtgesellschaftlichen und regulatorischen Rahmen mit IT-Sicherheits- und Datenschutz-Management-Glossar (Thomas A. Degen).....	43
1.1 Ausgangs-/Praxisfall	43
1.2 Risikomatrix	45
1.3 Cyberkriminalität und Verhaltensbotschaften für die Praxis	45
1.4 Informatik-/IT-Security-Fachbegriffe und Marketing-Buzzwords.....	51
1.5 Kurzübersicht der Rechtsquellen und der regulatorischen Anforderungen.....	52
1.5.1 Datenschutzregulierung	53
1.5.2 Beweisrecht und elektronische Signaturen.....	56
1.5.3 Zahlungsverkehr.....	56
1.5.4 Digitalisierung, Aufbewahrung und Beweisrecht.....	56
1.6 Verantwortung der Geschäftsleitung	57
1.7 Verantwortung der IT-Leitung und IT-Sicherheitsabteilung	58
1.8 Verantwortung des Datenschutzbeauftragten	58
1.9 Verantwortung der Personalabteilungsleitung.....	59
1.10 Verantwortung der Finanz-/Buchhaltungsabteilungsleitung.....	59
1.11 Verantwortung der Revisionsabteilungsleitung.....	60
1.12 Verantwortung der Vertriebsabteilungsleitung	60
1.13 Verantwortung der Marketingabteilungsleitung.....	60
1.14 Verantwortung des Betriebsrats	60
1.15 IT-Sicherheits- und Datenschutz-Management-Glossar ...	61
1.16 Zum Ausgangs-/Praxisfall.....	88

2.	IT-Sicherheit und Datenschutz (<i>Mathias Lang</i>).....	89
2.1	Ausgangs-/Praxisfall	89
2.2	Rechtsrahmen und Zuständigkeiten	90
2.2.1	Begriff der IT-Sicherheit.....	90
2.2.2	IT-Sicherheitsgesetz(e) und Gesetz zur Umsetzung der NIS-Richtlinie (EU) 2016/1148	92
2.2.3	DSGVO.....	94
2.2.4	Stand der Technik	97
2.2.5	Haftung und Sanktionen	105
2.2.6	Verantwortung	106
2.3	Praxishinweise	107
2.3.1	IT-Sicherheitsbeauftragter	107
2.3.2	Website – Sicherheitsüberprüfung.....	107
2.3.3	Datenverschlüsselung, Anonymisierung und Pseudonymisierung.....	108
2.3.4	Data protection by design und Data protection by default	108
2.3.5	DSFA.....	108
2.4	Gestalterische Empfehlungen und Compliance.....	108
2.4.1	Umsetzung – Stand der Technik.....	108
2.4.2	Zertifizierung?.....	109
2.4.3	Überwachung, Fehlerbeseitigung und Verbesserung.....	110
2.5	Zum Ausgangs-/Praxisfall.....	110
3.	Cross-border Datentransfer (<i>Jochen Deister/Ulrich Emmert/Thomas A. Degen</i>).....	111
3.1	Ausgangs-/Praxisfall	111
3.2	Rechtsrahmen und Zuständigkeiten	111
3.3	Zulässigkeit der Verarbeitung im Ausland	112
3.4	Verarbeitung von Beschäftigtendaten in der DSGVO	112
3.5	Das Bundesdatenschutzgesetz.....	113
3.5.1	Weite Definition der Beschäftigten	114
3.5.2	Rechtfertigung der Verarbeitung.....	114
3.5.3	Anstellungsvertrag und Kollektivvereinbarung.....	114
3.5.4	Einwilligung	115
3.5.5	Besondere Kategorien von Daten	116
3.6	Weitere Regelungen.....	117
3.7	Zusammenfassung.....	117
3.8	Angemessenes Schutzniveau.....	118
3.8.1	Angemessenheitsbeschluss	119
3.8.2	Sicheres Drittland.....	119
3.8.3	Privacy Shield (bis 2020)	121
3.8.4	Datenübermittlung vorbehaltlich geeigneter Garantien.....	122

3.8.5	Verbindliche interne Datenschutzvorschriften	123
3.8.6	Standardvertrags- bzw. Datenschutzklauseln.....	126
3.8.7	Verantwortlicher an Verantwortlichen (C2C)	126
3.8.8	EUMC C2C 2001	127
3.8.9	EUMC C2C 2004	127
3.8.10	Verantwortlicher an Verarbeiter (C2P).....	128
3.8.11	Verarbeiter an Verarbeiter (P2P).....	132
3.8.12	Änderungen durch die DSGVO	133
3.8.13	Standarddatenschutzklauseln.....	134
3.8.14	(Neue) Anwendungsfälle.....	134
3.8.15	Aufbau / Modularität.....	135
3.8.16	Inhaltliche Änderungen	135
3.8.17	Umsetzungszeitraum	137
3.9	Sonderfall Brexit	137
3.10	Zusammenfassung.....	138
3.11	Änderung nach Redaktionsschluss	139
4.	Digitalisierungsprojekte: Digitale Umstrukturierung im Unternehmen (Mathias Lang/Ulrich Emmert)	141
4.1	Ausgangs-/Praxisfall	141
4.2	Rechtsrahmen und Zuständigkeiten	142
4.2.1	Einführung.....	142
4.2.2	Digitales Dokumenten-Management.....	144
4.2.3	Digitale Rechnungstellung und Buchhaltung	146
4.2.4	Outsourcing und Digitalisierung der Arbeitsplätze.....	149
4.2.5	Collaboration-Tools	152
4.2.6	Cloud Computing und Cloud-Server	153
4.2.7	Videokonferenzen.....	153
4.2.8.	Zuständigkeiten.....	154
4.3	Praxishinweise	155
4.3.1	Richtlinien	155
4.3.2	BYOD oder firmeneigene Lösungen.....	158
4.3.3	Mobile Endgeräte.....	159
4.3.4	Collaboration-Tools	159
4.3.5	Videokonferenzen.....	159
4.3.6	Komplett-Lösungen	165
4.3.7	Datenschutz und Digitalisierung in der Pandemie	165
4.3.8	Lockerung von Rechtsvorschriften hinsichtlich der Pandemie.....	167
4.4.	Gestalterische Empfehlungen und Compliance.....	170
4.4.1	Richtlinien zu Homeoffice	170
4.4.2	Betriebsvereinbarung.....	174
4.4.3	Arbeitsvertraglicher Zusatz Homeoffice.....	178

4.4.4	Kombilösung für Arbeitsvertrag und Betriebsvereinbarung.....	183
4.4.5	Richtlinie für Mobile Geräte	187
4.5	Zum Ausgangs-/Praxisfall.....	189
5.	Digitalisierung, digitaler Vertrieb und E-Commerce-Projekte (Thomas Lapp)	191
5.1	Ausgangs-/Praxisfall	191
5.2	Rechtsrahmen und Zuständigkeiten	192
5.2.1	Formvorschriften/Schriftform.....	192
5.2.2	Sichere Kommunikation	194
5.2.3	Funktionen der Unterschrift	195
5.2.4	Gesetzliche Formvorschriften	195
5.2.5	Vertragliche Formvorschriften	196
5.2.6	Dokumentationspflichten.....	196
5.2.7	Hinderungsgründe gegen die Nutzung elektronischer Signaturen	196
5.3	Vertrauensdienste für elektronische Transaktion	197
5.3.1	Elektronische Signaturen	197
5.3.2	Fortgeschrittene elektronische Signaturen.....	197
5.3.3	Qualifizierte elektronische Signatur	198
5.3.4	Äquivalent zur eigenhändigen Unterschrift.....	199
5.3.5	Beweiswert qualifizierter elektronische Signaturen.....	199
5.3.6	Rechtswirkung und Beweiswert anderer elektronischer Signaturen	200
5.3.7	Fernsignaturen.....	201
5.3.8	Elektronisches Siegel.....	202
5.4	Praxishinweise	203
5.4.1	Digitalisierung bei formbedürftigen Rechtsgeschäften	203
5.4.2	Keine Weitergabe von PIN.....	205
5.4.3	Validierung	206
5.4.4	Archivierung.....	207
5.5	Gestalterische Empfehlungen und Compliance.....	207
5.5.1	Digitaler Workflow.....	207
5.5.2	Signatur ist keine Unterschrift.....	208
5.5.3	Akzeptanz	208
6.	Web-Projekte: Website-Erstellung und Relaunch (Mathias Lang).....	209
6.1	Ausgangs-/Praxisfall	209
6.2	Rechtsrahmen und Zuständigkeiten	210
6.2.1	Einführung.....	210
6.2.2	Domainrecht	211

6.2.3	Designrecht	211
6.2.4	Impressumpflicht	213
6.2.5	Datenschutz	214
6.2.6	Urheberrecht (Texte, Bilder, Videos)	221
6.2.7	KUG-Recht am eigenen Bild, Verhältnis zum Datenschutz	222
6.2.8	E-Commerce.....	223
6.2.9	Wettbewerbsrecht	228
6.2.10	IT-SiG bzw. TTDSG.....	231
6.2.11	Verantwortlichkeit.....	231
6.3	Praxishinweise	232
6.3.1	Domainauswahl- und Registrierung	232
6.3.2	Designauswahl.....	232
6.3.3	Impressumsgestaltung	233
6.3.4	Datenschutzgestaltung	233
6.3.5	Urheberrecht.....	236
6.3.6	Mitarbeiterbilder.....	237
6.3.7	E-Commerce.....	237
6.4	Gestalterische Empfehlungen und Compliance.....	242
6.4.1	Hinweispflichten zur Alternativen Streitbeilegung.....	242
6.4.2	Newsletter.....	243
6.4.3	Cookie-Banner oder Consent-Tool?	243
6.4.4	IT-SiG	244
6.4.5	Verantwortlichkeit.....	244
6.5	Zum Ausgangs-/Praxisfall.....	245
7.	Social Media-Projekte: Arbeit und Social Media	
	<i>(Mathias Lang)</i>	247
7.1	Ausgangs-/Praxisfall	247
7.2	Rechtsrahmen und Zuständigkeiten	248
7.3	Praxishinweise	251
7.4	Gestalterische Empfehlungen und Compliance.....	252
7.4.1	Arbeitsvertrag (Zusatz)	252
7.4.2	Betriebsvereinbarung.....	253
7.4.3	Einwilligungserklärung	259
7.4.4	Social-Media-Manager Vertrag	260
7.4.5	Social-Media-Guidelines.....	261
7.5.	Zum Ausgangs-/Praxisfall.....	263
8.	Digitaler Vertrieb, Nachverfolgung, Services über IoT,	
	Mobilität (Jochen Deister)	265
8.1	Ausgangs-/Praxisfall	265
8.2	Rechtsrahmen und Zuständigkeiten	265
8.2.1	Einführung.....	265

8.2.2	Die Behandlung innovativer Technologien in der DSGVO	267
8.3	Praxishinweise	282
8.4	Gestalterische Empfehlungen und Compliance.....	283
9.	Agile Projekte, Scrum, F&E & Datenschutz <i>(Thomas A. Degen)</i>	285
9.1	Ausgangs-/Praxisfall	285
9.2	Rechtsrahmen und Zuständigkeiten	286
9.2.1	Grundsätzliche Hinweise zur Projekt- umsetzungen und Vertragsgestaltungen im IT-Business.....	286
9.2.2	Gestaltungsformen bei der Softwareüber- lassung auf Dauer	289
9.2.3	Softwareüberlassung und Open Source- Produkte.....	290
9.2.4	Leistungsbeschreibung Teil 1 – „Was kann das Programm?“	292
9.2.5	ASP und „Web Service“	293
9.2.6	Vom Wasserfallmodell zu agilen Verfahrens- modellen wie KANBAN, Scrum, XP, Spiralmodell, MDA, RUP & Co.	294
9.2.7	Rechtsrahmen bei agiler Software- entwicklung nach Scrum	297
9.2.8	Vertragsrechtliche Leistung (Teil 2) und Qualifizierung von agilen Projekten nach Scrum.....	300
9.3	IT- und Datenschutz-Compliance- und Gestaltungs- hinweise wegen erhöhter Projektrisiken bei agilen Methoden wie Scrum.....	305
9.4	Datenschutzrechtliche Besonderheiten bei Scrum.....	316
9.5	Zum Ausgangs-/Praxisfall.....	318
9.6	Annex: Agile Fehlervermeidung bei F&E- und Scrum-Projekten – Perspektivwechsel zu IT-Sachverständigen und Richtern.....	320
10.	Cloud- und SaaS-Verträge <i>(Ulrich Emmert/Thomas A. Degen)</i>	325
10.1	Ausgangs-/Praxisfall	325
10.2	Vorteile und Aufbau einer Cloud-Infrastruktur	325
10.3	Vertragliche Situation bei Cloudverträgen	329
10.3.1	Einflussmöglichkeiten der Vertragsgestaltung	329
10.3.2	Vertragstypen des Bürgerlichen Gesetzbuches.....	330
10.4	Gesetzliche Gewährleistung bei Cloud-Verträgen	332

10.5	Übersicht über die verschiedenen Gewährleistungsrechte.....	333
10.6	Vertragliche Regelungsbereiche.....	334
10.6.1	Wie viele Vertragsparteien gibt es und welche Leistungen übernehmen sie?.....	334
10.6.2	Welches nationale Recht gilt für welche Rechte und Pflichten?.....	334
10.6.3	Wer hat Zugriff auf welche Leistungen und welche Daten?.....	335
10.6.4	In welchem Land werden Leistungen erbracht und die Daten gespeichert?	336
10.6.5	Wie werden Änderungen im Bedarf umgesetzt und was geschieht bei Abweichungen in der Vertragserfüllung?.....	336
10.6.6	Wie wird die Vergütung für welche Leistungen berechnet?.....	337
10.6.7	Wie werden spezifische rechtliche Anforderungen und interne Vorgaben des Kunden umgesetzt?.....	337
10.6.8	Wie werden Störungen der Leistung rechtlich bewertet?	338
10.7	Regelungen in zugehörigen Service Level Agreements.....	338
10.7.1	Verfügbarkeit des Systems oder Dienstes in einem bestimmten Messzeitraum.....	338
10.7.2	Wartungszeiträume.....	339
10.7.3	Reaktionszeiten auf Mängelmitteilung.....	339
10.7.4	Umgehungs- oder Beseitigungszeiten bei Mängeln	339
10.7.5	Mindestleistungsdaten	340
10.7.6	Change Management und Bearbeitungszeiten.....	340
10.7.7	Datensicherheit.....	340
10.7.8	Migrationsleistungen bei Wechsel des Providers	341
10.7.9	Kündigungsfristen	341
10.7.10	Leistungen am Vertragsende	341
10.7.11	Konfliktregelungen	342
10.8	Internationaler Datenschutz bei Cloudsystemen	342
10.9	Empfehlungen zur Auswahl von Cloudsystemen	343
	Zum Ausgangs-/Praxisfall.....	343

11. Aspekte des Urheberrechts bei Medien-Projektumsetzungen mit fremden Texten, Bildern, Vorlagen, Kartenmaterial (<i>Ulrich Emmert/Thomas A. Degen</i>)	345
11.1 Ausgangs-/Praxisfall	345
11.2 Hinweise zum Urheberrecht bei Nutzung von Vorlagen, Medien und Kartenmaterial	345
11.3 Nutzung und Verwertung fremder Vorlagen und Leistungen	346
11.4 Nutzung von Bildern.....	348
11.5 Kartenmaterial.....	353
a. Openstreetmap.....	353
b. Google Maps	354
c. Geodatenviewer BW	355
11.6 Abbildungen von Personen	356
11.7 Nutzung von audiovisuellen Medien.....	356
11.8 Nutzung von Social Media	358
11.9 Verletzung fremder Markenrechte.....	359
11.10 Verletzung des Wettbewerbsrechts.....	360
11.11 Zum Ausgangs-/Praxisfall.....	360
12. IT-Beschaffung, Hardware- und Software-Einkauf (<i>Ulrich Emmert/Thomas A. Degen</i>).....	361
12.1 Ausgangs-/Praxisfall	361
12.2 Rechtsrahmen und Zuständigkeiten	363
12.3 Praxishinweise, technische, organisatorische Maßnahmen.....	368
12.4 Gestalterische Empfehlungen und Compliance.....	368
12.5 Lizenzrechtliche Besonderheiten bei der IT-Beschaffung.....	368
12.5.1 ERP-Software nebst Web- und Mobile App-Schnittstelle.....	369
12.5.2 Lizenzrecht in der Praxis: MS, SAP, Oracle	369
12.5.3 Indirekte Nutzung.....	370
12.5.4 Netweaver	370
12.5.5 Gestalterische Empfehlungen und Compliance.....	371
12.6 Besonderheiten im IT-Einkauf im Bauwesen mit Digitalisierung von Geschäftsprozessen und Dokumenten	371
12.6.1 Building Information Modeling.....	371
12.6.2 Rechtsrahmen und Zuständigkeiten.....	372
12.6.3 Archivierungspflichten und Praxishinweise, technische, organisatorische Maßnahmen	374

13	IT-Konfliktmanagement (<i>Thomas Lapp</i>).....	377
13.1	Ausgangs-/Praxisfall	377
13.2	Rechtsrahmen und Zuständigkeiten	377
13.2.1	Rechtsrahmen: Kaufvertrag oder Werkvertrag.....	377
13.2.2	Change Request.....	378
13.2.3	Exit.....	379
13.2.4	Eskalation.....	379
13.3	Praxishinweise	380
13.3.1	Change Request (CR)	380
13.3.2	Exit	381
13.3.3	Eskalation.....	382
13.4	Gestalterische Empfehlungen und Compliance.....	398
13.4.1	Change Request.....	398
13.4.2	Exit	399
13.4.3	Eskalationsklauseln	399
13.5	Zum Ausgangs-/Praxisfall.....	401
14	IT-Sicherheitsaspekte bei der elektronischen Kommunikation, Authentizität, Identität und Beweiswerterhaltung mit kryptographischen Verfahren (<i>Ulrich Emmert/Thomas A. Degen</i>)	403
14.1	Ausgangs-/Praxisfall	403
14.2	Verschlüsselung und digitale Signaturen	404
14.3	Funktionsweise von 2-Schlüsselverfahren	407
14.4	Anwendung von Verschlüsselung im deutschen Rechtsverkehr.....	410
14.5	Beweiswerterhaltung mit Verkettung von Hashwerten und digitalen Signaturen	411
14.6	Beweiswerterhaltung bei ersetzendem Scannen	414
14.7	Zum Ausgangs-/Praxisfall.....	415
	Abbildungsverzeichnis	417
	Stichwortverzeichnis	421